

(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020010050381 A
 (43)Date of publication of application: 15.06.2001

(21)Application number: 1020000053161
 (22)Date of filing: 07.09.2000
 (30)Priority: 17.09.1999 US 1999 397419
 (51)Int. Cl. G06F 17/60

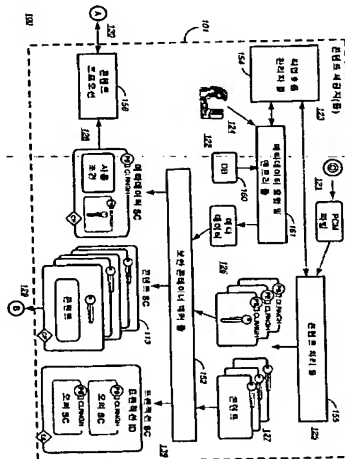
(71)Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION
 (72)Inventor: DORACK JR. JOHN J.

(54) METHOD AND DEVICE FOR UNIQUELY IDENTIFYING CUSTOMER PURCHASE IN ELECTRONIC DISTRIBUTION SYSTEM

(57) Abstract:

PURPOSE: To provide a system for tracing the use of digital contents on a user device.

CONSTITUTION: A content site distributes digital contents via a computer-readable medium to a user. The content site relates a unique content identifier with the related contents. An electronic store connected with a network sells a license for reproducing the digital content data to the user. The license includes the unique item identifier for uniquely identifying at least one item in the transaction. Then, a content player which receives the content data given the license from the network, is used for the reproduction of the content data given the license. The content player prepares a purchase identifier, based on the mathematical combination of the content identifier, the transaction identifier, and the item identifier.



© KIPO & JPO 2002

Legal Status

Best Available Copy

(19)대한민국특허청(KR)
(12) 공개특허공보(A)(51) Int. Cl. ⁶
G06F 17/60A2(11) 공개번호 특2001-0050381
(43) 공개일자 2001년06월15일

(21) 출원번호 10-2000-0053161

(22) 출원일자 2000년09월07일

(30) 우선권주장 09039741901999년09월17일미국(US)

(71) 출원인 인터내셔널 비지네스 머신즈 코포레이션 포만 제프리 엘
미국 10504 뉴욕주 아몬크(72) 발명자 도락,존제이,쥬니어
미국플로리다33428,보카라톤,사우스웨스트62번애버뉴22238(74) 대리인 신영무
최승민
윤혜진
조인제

심사청구 : 있음

(54) 전자 배포 시스템에서 고객 구매를 유일하게 식별하기 위한 방법 및 장치

요약

사용자 장치에서의 디지털 콘텐츠의 사용을 추적하기 위한 시스템이 제공된다. 디지털 콘텐츠를 컴퓨터 판독가능 매체를 거쳐 사용자에게 배포하기 위한 콘텐츠 사이트가 제공된다. 콘텐츠 사이트는 유일 콘텐츠 식별자를 이와 연관된 콘텐츠와 연관시킨다. 네트워크와 결합된 전자 스토어는 디지털 콘텐츠 데이터를 플레이하기 위한 인가(license)를 사용자에게 판매한다. 인가는 트랜잭션을 유일하게 식별하기 위한 유일 트랜잭션 식별자를 포함하며, 인가는 트랜잭션에서의 적어도 하나의 아이템을 유일하게 식별하기 위한 유일 아이템 식별자를 포함한다. 인가된 콘텐츠 데이터를 네트워크로부터 수신하는 콘텐츠 플레이어는 인가된 콘텐츠 데이터를 플레이하기 위해 이용된다. 콘텐츠 플레이어는 콘텐츠 식별자, 트랜잭션 식별자 및 아이템 식별자의 수학적 조합에 기초하여 구매 식별자를 생성한다.

대표도

도1a

색인어

식별자, 트랜잭션, 보안 컨테이너, 콘텐츠 제공자, 전자 디지털 콘텐츠 스토어, 클리어링하우스

명세서

도면의 간단한 설명

도 1a 내지 도 1d는 본 발명에 따른 보안 디지털 콘텐츠 전자 배포 시스템의 개요를 예시한 블록도이다.

도 2는 본 발명에 따른 예시적 보안 컨테이너(SC) 및 연관된 그래픽적 표현을 예시한 블록도이다.

도 3은 본 발명에 따른 보안 컨테이너(SC)에 대한 암호화 처리의 개요를 예시한 블록도이다.

도 4는 본 발명에 따른 보안 컨테이너(SC)에 대한 해독화 처리의 개요를 예시한 블록도이다.

도 5는 본 발명에 따른 도 1의 보안 디지털 콘텐츠 배포 시스템의 권리 관리 구조에 대한 층의 개요를 예시한 블록도이다.

도 6은 도 5의 인가(license) 제어층에 적용함에 따른 콘텐츠 배포 및 인가 제어의 개요를 예시한 블록도이다.

도 7은 본 발명에 따른 도 1의 워크 플로우 관리 틀에 대한 일례의 사용자 인터페이스를 예시한다.

도 8은 본 발명에 따른 도 7에서의 사용자 인터페이스에 대응하는 워크 플로우 관리자의 처리, 성분 및 주요 틀을 예시한 블록도이다.

도 9는 본 발명에 따른 도 1의 전자 디지털 콘텐츠 스토어의 처리, 성분 및 주요 틀을 예시한 블록도이다.

도 10은 본 발명에 따른 도 1의 최종 사용자 장치(들)의 처리 및 주요 성분을 예시한 블록도이다.

도 11은 본 발명에 따른 도 8의 압축 틀 및 콘텐츠 처리를 위한 인코딩 레이트 인자를 계산하기 위한 방법의 흐름도이다.

도 12는 본 발명에 따른 도 8의 자동 메타 데이터 취득 틀에 대한 부가 정보를 자동적으로 검색하기 위한 방법의 흐름도이다.

도 13은 본 발명에 따른 도 8의 전처리 및 압축의 전처리 및 압축 파라미터들을 자동적으로 설정하기 위한 방법의 흐름도이다.

도 14는 본 발명에 따른 도 15에서 설명되는 바와 같이, 로컬 라이브러리로 콘텐츠를 다운로드하는 플레이어 애플리케이션의 사용자 인터페이스 스크린의 일례이다.

도 15는 본 발명에 따른 도 9의 최종 사용자 장치상에서 실행하는 플레이어 애플리케이션의 처리 및 주요 성분을 예시한 블록도이다.

도 16은 본 발명에 따른 도 15의 플레이어 애플리케이션의 일례인 사용자 인터페이스 스크린이다.

도 17은 본 발명에 따른 도 8의 자동 메타 데이터 취득 틀에 대한 부가 정보를 자동으로 검색하기 위한 다른 실시예의 흐름도이다.

도 18은 본 발명에 따라 독립적으로 콘텐츠를 추적하기 위한 최종 사용자 장치(9)를 실행하는 처리의 흐름도이다.

※도면의 주요 부분에 대한 부호의 설명※

100: 보안 디지털 콘텐츠 전자 배포 시스템

101: 콘텐츠 제공자(들)

103: 전자 디지털 콘텐츠 스토어(들)

105: 클리어링하우스(들)

107: 전송 기반 시설

109: 최종 사용자 장치(들)(109)

111: 콘텐츠 호스팅 사이트

113: 콘텐츠

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야 종래기술

본 발명은 광범위하게는 전자 상거래 분야에 관한 것으로, 특히 인터넷 및 월드 와이드 웹(World Wide Web)과 같은 글로벌(global) 통신 네트워크를 통한 인쇄 매체, 영화, 게임 및 음악과 같은 디지털 자산의 보안 전송 및 권리 관리를 위한 시스템 및 관련 틀에 관한 것이다.

발명이 이루고자하는 기술적 과제

음악, 영화, 컴퓨터 프로그램, 화상, 게임 및 다른 콘텐츠와 같은 디지털 자산의 배포하기 위한 인터넷과 같은 글로벌 배포 시스템의 사용이 증가하고 있는 추세이다. 동시에 가치있는 디지털 콘텐츠의 소유자 및 제작자는 몇 가지 이유로 인하여 디지털 자산의 배포를 위해 인터넷을 이용하는 것을 서두르지 않고 있다. 한가지 이유는 콘텐츠 소유자가 디지털 콘텐츠의 허가받지 않은 복사 또는 불법 복제를 걱정한다는 것이다. 디지털 콘텐츠의 전자 전달은 불법 복제를 방지하는 장애물이 없다. 전자 배포분에서 제거되는 한가지 장애물은 유형의 기록가능한 매체(예를 들면, 디스켓 또는 CD ROM)이다. 많은 경우에, 공 테이프 또는 기록가능한 CD를 구입하기 위해 1 달러 이하의 돈을 들여야 하는 것과 같이, 유형의 매체상에 디지털 콘텐츠를 복사하는 데에는 비용이 든다. 그러나, 전자 배포의

경우에, 유형 매체는 더 이상 필요하지 않다. 콘텐츠가 전자적으로 배포되기 때문에 유형 매체를 구입하는 데 드는 비용이 필요없다. 두 번째 장애물은 콘텐츠 그 자체의 포맷으로서, 즉 아날로그 포맷 대 디지털 포맷으로 저장되는 콘텐츠이다. 아날로그 포맷으로 저장된 콘텐츠, 예를 들면, 프린트된 화상은, 복사물을 사진 복사하여 재생될 때 원본보다 질이 떨어진다. 복사물을 연속하여 각각 복사한 것, 소위 재생은 원본보다 질이 떨어진다. 이러한 질의 저하는 화상이 디지털적으로 저장될 때는 발생하지 않는다. 디지털적으로 저장될 때 각각의 복사물 및 복사물의 모든 재생은 원본 만큼 선명할 것이다. 콘텐츠를 전자적으로 인터넷을 통해 널리 배포시키기 위해 매우 낮은 비용으로 연결된 완전한 디지털 복사물의 집합적 효과는 허가받지 않은 복사물을 불법 복사하고 배포시키는 것을 비교적 쉽게 한다. 키를 두 번 치면, 인터넷을 통해 디지털 콘텐츠의 수백 또는 심지어 수천의 완전한 복사물이 불법 복사물로서 전송될 수 있다. 그러므로, 전자적으로 배포되는 디지털 자산의 보호와 보안을 확실하게 할 필요가 있다.

디지털 콘텐츠의 제공자는 콘텐츠 소유자의 권리를 보호하는 디지털 콘텐츠를 위한 보안성의 글로벌 배포 시스템을 도입하고 싶어한다. 디지털 콘텐츠 배포 시스템을 도입하는 데에 있어서의 문제점은 디지털 콘텐츠 전자 배포, 권리 관리 및 자산 보호를 위한 개선된 시스템이 필요하다는 것이다. 전자적으로 배포되는 디지털 콘텐츠는 프린트 매체, 영화, 게임, 프로그램, 텔레비전, 멀티미디어 및 음악과 같은 콘텐츠를 포함한다.

전자 배포 시스템을 사용하면 콘텐츠의 재배포를 통해 재고품의 2차적 소득원은 물론 직접적 판매 보고 및 전자적 조정을 통한 빠른 지불 처리를 성취하는 기능을 디지털 콘텐츠 제공자에게 제공한다. 전자 디지털 콘텐츠 배포 시스템은 물리적 재고품 감량 또는 반품에 의해 영향을 받지 않기 때문에, 디지털 콘텐츠 제공자와 소매업자는 비용 감소와 이익 증대를 실현할 수 있다. 디지털 콘텐츠 제공자는 재고품의 더 양호한 정기적 방출을 위한 새로운, 또는 기존에 있던 배포 채널을 편리하게 할 수 있다. 전자 배포 시스템으로부터의 트랜잭션 데이터는 전자 마케팅 프로그램 및 광고에 직접적 피드백을 제공하는 것은 물론 소비자 구매 패턴에 대한 정보를 얻기 위해 사용될 수 있다. 이러한 목적에 부합하기 위해, 디지털 콘텐츠 제공자는 광범위한 사용자와 비즈니스에 사용가능한 디지털 콘텐츠를 구성하고 동시에 디지털 자산의 보호와 미터링(metering)을 보장하는 전자 배포 모델을 이용할 필요가 있다.

리얼 오디오, AT & T사에서 생산된 A2B, Liquid Audio Pro 사에서 생산된 Liquid Audio Pro, Audio Soft사에서 생산된 City Music Network 등과 같은 디지털 콘텐츠를 위한 다른 상업적으로 사용가능한 전자 배포 시스템은 보안성 및 비보안성 통신 네트워크를 통해 디지털 데이터를 전송한다. 보안성 전자 네트워크를 사용하면 광범위한 고객에게 디지털 데이터를 배포하고자 하는 디지털 콘텐츠 제공자의 요구에 부합하지 못한다. 그러나, 인터넷과 웹과 같은 비보안성 네트워크를 사용하여 암호의 사용 등을 통해 최종 사용자에게 디지털 콘텐츠를 보안성있게 전달시킬 수 있다. 그러나, 암호화된 디지털 콘텐츠가 최종 사용자의 기계상에서 암호해독되면, 디지털 콘텐츠는 최종 사용자에게 의해 허가받지 않은 재배포를 위해 쉽게 사용가능하다. 그러므로, 디지털 자산을 보호하고, 콘텐츠 제공자(들)의 권리가 심지어 디지털 콘텐츠가 소비자와의 사업으로 전달된 후에도 보호되도록 보장할 수 있는 보안성 디지털 콘텐츠 전자 배포 시스템이 필요하다. 그러므로, 보안성 전송, 인가 허가 및 디지털 자산의 사용 제어를 가능하게 하기 위한 권리 관리가 필요하다.

디지털 콘텐츠의 소유자가 전자 배포 시스템을 도입하는 데에 서두르지 않는 다른 이유는 기존의 배포 채널을 관리하고 육성하고자 하기 때문이다. 대부분의 콘텐츠 소유자는 소매 업자를 통해 판매한다. 음악 마케팅에서 이러한 U.S. 소매 업자는 Tower Records, Peaches, Blockbuster, Circuit City 등을 포함한다. 이러한 소매 업자 대부분은 인터넷 사용자가 인터넷을 통해 선택하여 최종 사용자에게 메일을 통해 선택하게 하는 웹 사이트를 소유하고 있다. 예시적인 음악 웹 사이트는 @tower, Music Boulevard 및 Columbia House를 포함한다. 전자 배포의 사용은 소매 스토어들이 그들의 스토어를 다른 스토어들과 차별화시키는 수고를 필요없게 할 수 있고 그들 스토어를 특히 웹상에서 다른 콘텐츠 소유자와 차별화시킨다. 그러므로, 배포를 통해 음악을 판매할 때 화상, 게임, 음악, 프로그램 및 비디오와 같은 전자 콘텐츠의 소매 업자에게 그들의 콘텐츠를 다른 콘텐츠와 서로 차별화시키기 위한 방법을 제공할 필요가 있다.

콘텐츠 소유자는 전자 스토어와 같은 배포 사이트를 통한 전자 배포를 위해 그들의 디지털 콘텐츠를 준비한다. 인터넷, 또는 다른 온라인 서비스를 통한 전자 스토어는 그들의 제품의 제공 및 제품 선택에 의해 그들의 제품을 다른 제품들과 차별화시키고 싶어한다. 종래의 스토어, 즉, 온라인 스토어와 비교하여 통신을 이용하지 않는, 온라인을 통하지 않는 아날로그 방식의 스토어들은 그들의 제품을 경쟁상대들과 차별화시키기 위해 제품 광고, 제품 세일, 제품 샘플, 자유 반품 정책 및 다른 판매 촉진 프로그램을 사용한다. 그러나, 콘텐츠 제공자가 디지털 콘텐츠상에 사용 조건을 부여하는 온라인 상에서, 그들의 제품을 차별화시키는 통신 스토어의 능력은 엄격하게 제한될 수 있다. 더우기, 사용 조건이 변경할 수 있다고 하더라도, 전자 스토어는 콘텐츠 제공자가 제품을 전자 배포를 통해 광고하고 판매하기 위해서 디지털 콘텐츠와 연결된 메타 데이터(metadata)를 처리하는 어려운 작업에 직면하게 된다. 전자 스토어는 메타 데이터를 처리할 때, 몇 가지 요구를 관리할 필요가 있다. 첫 번째로, 전자 스토어는 디지털 콘텐츠와 연결된 메타 데이터를 콘텐츠 제공자로부터 수신할 필요가 있다. 여러번 이러한 메타 데이터의 일부분이 암호화되어 보내지면, 콘텐츠 제공자는 암호화된 콘텐츠를 해독하기 위한 매커니즘을 생성해야 한다. 둘째로, 전자 스토어는 콘텐츠가 콘텐츠 제공자로부터 수신되기 전에, 또는 콘텐츠가 전자 스토어에 의해 수신된 후에 제품 마케팅, 제품 포지셔닝 및 콘텐츠를 위한 다른 프로모션을 보조하기 위해 콘텐츠 제공자로부터 메타 데이터를 사전검토하고 싶어한다. 세째로, 전자 스토어는 그래픽 및 예술가 정보와 같은 프로모션 자료에 사용되는 어떤 메타 데이터를 추출할 필요가 있다. 흔히, 이러한 프로모션 자료는 온라인 광고시에 전자 스토어에 의해 직접 사용된다. 네째로, 전자 스토어는 디지털 콘텐츠의 다른 판매를 생성하기 위해 허가된 사용 조건중 일부를 변경시킴으로써 그들을 서로 차별화시키고 싶어한다. 다섯째로, 전자 스토어는 지불 처리를 위해 전자 스토어를 이용할 필요없이 구매자에 의해 자동으로 계좌 관리원에 지불 처리를 지시하기 위해서 메타 데이터에서 URL과 같은 어떤 어드레스를 삽입하거나 변경시켜야만 한다. 여섯째로, 전자 스토어는 사용 조건을 맞추는 저작권이 보호된 디지털 콘텐츠의 허가된 사용을 위한 인가를 생성할 필요가 있다. 예를 들면, 이 인가는 디지털 콘텐츠의 제한된 횟수의 복사물을 생성하기 위한 허가권을 부여한다. 인가는 부여된 허가권의 기간과 조건을 나타내기 위해 필요하다.

이러한 모든 요구면에서, 디지털 콘텐츠와 관련된 메타 데이터를 처리하기 위해서, 많은 전자 스토어가 이러한 요구들을 처리하기 위한 개별화된 소프트웨어 프로그램을 기록한다. 이러한 개별화된 소프트웨어 프로그램을 생성하기 위해 필요한 시간, 비용 및 테스트

은 대용량일 수 있다. 따라서, 이러한 요구에 대한 해결책을 제공할 필요가 있다.

아직까지, 디지털 콘텐츠의 소유자가 전자 배포를 위한 콘텐츠를 도입하는 데에 서두르지 않는 다른 이유는 전자 배포를 위한 콘텐츠를 준비하는 것이 어렵기 때문이다. 오늘날, 많은 콘텐츠 제공자는 그들의 포트폴리오에서 수 천개의 또는 심지어 수 억개의 타이틀을 갖는다. 음악 사이트를 예로 들면, 콘텐츠 소유자가 몇몇의 다른 포맷으로 동시에(예를 들면, CD, 테이프 및 미니디스크) 사용 가능한 단일 마스터 사운드 녹음을 하는 것은 흔한 일이다. 또한, 단일 포맷은 특정한 배포 채널을 위해 리마스터(re-mastered)되거나 리믹스(re-mixed)된 마스터 사운드 녹음을 할 수 있다. 예를 들면, 방송 라디오를 위한 믹싱은 댄스 클럽 사운드 트랙용의 믹싱과는 다르며, 일반적으로 사용되는 소비자용 CD와도 다르다. 이러한 다른 믹스의 목록 작성 및 트랙 관리는 부담스러운 것이다. 또한, 많은 마스터 녹음의 소유자는 흔히 "The Best Of"와 같은 다양한 후속 컬렉션에서, 또는 영화의 뮤직 사운드 트랙을 위한 편집을 및 다른 컬렉션 또는 편집물에서 재발행된 예전의 녹음의 시간을 맞춘다. 더 많은 콘텐츠가 디지털적으로 제공되고 있기 때문에, 전자 배포를 위한 콘텐츠를 리믹스하고 암호화할 필요성은 증가하고 있다. 많은 경우에, 콘텐츠 제공자는 올바른 마스터 사운드와 올바른 녹음을 선택하고 전자 배포를 위한 발행을 위해 재처리되고 암호화된 이러한 사운드 녹음을 하기 위해 가이드로서 종래의 녹음 포맷을 사용할 필요가 있다. 이것은 전자 배포를 위해 종래의 사운드 녹음을 재발행할 때 이들을 돕기 위해 종래의 포맷을 사용하고자 하는 콘텐츠 제공자를 위해 특히 유용하다. 제공자는 암호화 파라미터를 설정하기 위해 타이틀, 가수 및 사운드 녹음을 맞추기 위해 데이터베이스를 검사한다. 포트폴리오를 녹음을 하기 위해 수동적으로 데이터베이스를 검색하는 이러한 처리는 단점을 가지고 있다. 한 가지 단점은 조작자에게 데이터베이스를 수동으로 검색하도록 하고 프로세스 파라미터를 적당하게 설정할 필요가 있다는 것이다. 다른 단점은 데이터베이스에서 데이터를 선택할 때 조작자 복사 에러가 발생할 수 있다는 것이다. 따라서, 오디오와 같은 콘텐츠를 위한 관련 데이터 및 마스터 녹음을 자동으로 복구시키는 방법을 콘텐츠 제공자에게 제공할 필요가 있다.

콘텐츠 소유자는 암호화로 알려진 처리를 통해 전자 배포를 위한 디지털 콘텐츠를 준비한다. 암호화는 콘텐츠를 선택하는 단계 및 그 콘텐츠를 디지털화하는 단계, 콘텐츠가 아날로그 포맷으로 제공될 때 그 콘텐츠를 압축하는 단계를 포함한다. 압축하는 프로세스는 전송되거나 저장된 데이터의 양이 감소되기 때문에 네트워크상으로 전송되고 판독가능한 매체상에 저장되는 디지털 콘텐츠가 더욱 효율적으로 운영되도록 한다. 그러나, 압축에도 단점이 있다. 대부분의 압축은 어떤 정보의 손실을 포함하고 손실을 가진 압축으로 불린다. 콘텐츠 제공자는 어떤 압축 알고리즘이 사용되는 지와 요구되는 압축 레벨을 결정해야 한다. 예를 들면, 음악에서, 디지털 콘텐츠 또는 노래는 음악의 종류에 따라 매우 다른 특성을 갖는다. 한가지 종류에 대해 선택된 압축 알고리즘과 압축 레벨은 또다른 종류의 음악에 대해서는 최적의 선택이 아닐 수 있다. 콘텐츠 제공자는 압축 알고리즘의 어떤 결합이 음악의 한 종류, 말하자면 클래식 음악 등에 대해 매우 잘 동작하지만, 헤비 메탈과 같은 다른 종류의 음악에 대해서는 만족스럽지 못한 결과를 제공한다는 것을 알 수 있을 것이다. 또한, 오디오 엔지니어는 흔히 음악을 이퀄라이즈하고, 동적 범위 조정을 수행하며 다른 사전 처리 및 처리 설정을 수행하여 소망하는 결과를 생성하도록 그 음악의 종류를 암호화되도록 보장한다. 이퀄라이즈 레벨 설정과 다이내믹 레벨 설정과 같은 이러한 암호화 파라미터를 수동으로 항상 설정해야한다는 것은 부담스러운 것이다. 음악의 예로 돌아가서, 다양한 음악 종류를 포함한 컬렉션을 가진 음악의 콘텐츠 제공자는 암호화될 각각의 노래 또는 노래 세트를 수동으로 선택해야 한다. 따라서, 암호화를 위한 프로세스 파라미터를 수동으로 선택할 필요성을 없앨 필요가 있다.

콘텐츠를 압축하는 프로세스는 특히 완전한 길이의 영화와 같은 더 큰 콘텐츠 아이템을 위해 다량의 컴퓨터 자원을 필요로 한다. 압축 알고리즘의 제공자는 그들의 압축 기술과 관련된 여러가지 거래와 이점을 제공한다. 이러한 이점은 콘텐츠를 압축하는 데에 필요한 시간 총량 및 컴퓨터 자원; 원래의 콘텐츠로부터 얻어진 압축량; 재생을 위한 소망 비트 레이트; 압축된 콘텐츠의 성능 특징 및 다른 요소들을 포함한다. 멀티미디어 파일을 입력으로 선택하고 경과 또는 상황의 임시 지시 없이 암호화된 출력 파일을 생성하는 암호화된 프로그램을 사용하는 것은 문제가 있다. 또한, 많은 경우에, 경과와 임시 지시 없이 암호화 프로그램을 호출하거나 관리하기 위해 다른 프로그램이 사용된다. 이것은 암호화되는 것으로 지정된 전체 선택의 퍼센트로서 암호화된 콘텐츠의 양을 측정하는 수단없이 호출 애플리케이션을 남겨둔다. 한번 가동될 몇가지 다른 프로그램을 호출 프로그램이 스케줄링하려고 시도하는 경우에, 이러한 것이 문제가 될 수 있다. 또한, 이것은 콘텐츠의 배치가 암호화를 위해 선택되었으며 콘텐츠 제공자가 프로세스 암호화의 경과를 결정하고 싶어하는 경우에 특히 부담이 될 수 있다.

디지털 콘텐츠 제공자가 그들의 콘텐츠에 대한 전자 유통을 채택하는 것을 서두르지 않는 다른 이유는 사용자 장치상의 디지털 디스크 플레이어 생성하기 위한 기준이 부족하기 때문이다. 전자 배포 체인의 콘텐츠 제공자, 전자 스토어 등은 PCS, 셋톱 박스, 휴대용 장치 등과 같은 다양한 장치상에 개별화된 플레이어를 제공하고 싶어한다. 탬퍼 저항 환경에서 디지털 콘텐츠의 해독을 처리할 수 있는 한 세트의 툴, 즉, 제3 부분에 의해 동작하는 동안 콘텐츠에 대한 허가받지 않은 액세스를 거절하는 환경이 필요하다. 더욱이, 최종 사용자가 구매된 것과 다르게 사용하기 위한 콘텐츠에 대한 액세스를 갖지 않도록 하고 최종 사용자가 디지털 콘텐츠의 로컬 라이브러리를 관리할 수 있게 하는 한 세트의 툴이 필요하다.

디지털 콘텐츠의 배포에 있어서 콘텐츠 소유자가 직면하게 되는 다른 문제점은 구매 트랜잭션이 콘텐츠 동일 부분의 다중 복사물을 포함하고 있다는 것이다. 예를 들면, 고객이 하나의 복사를 할 권리를 가지고 하나의 노래 또는 하나의 음악을 구매하였다고 가정한다. 부가적으로, 고객은 더 이상의 복사를 할 권리 없이도 친구를 위해 그 노래의 2차적 선택권을 구매할 것을 결정한다. 노래의 구매자에게, 같은 노래의 동일한 복사를 혼란시키는 것은 쉽다. 이것은 콘텐츠 소유자가 하나의 노래에 대한 각각의 선택, 특히 동일한 노래를 찾아가고자 하기 때문에 바람직하지 않다. 노래들, 특히 동일한 노래를 찾아가고자 하는 요구는 동일한 노래 각각에 대한 사용 조건이 검색되어야 할 때 더욱 중요해진다. 더욱이, 다른 많은 수집물 또는 세트에서 동일한 노래가 방출되는 경우는 흔하다. 예를 들면, 동일한 노래는 단일 노래이거나, 앨범 또는 CD의 일부이거나, 대표 히트곡들 중의 일부 또는 셋톱 박스의 최신 부분일 것이다. 동일한 노래의 이와 같은 다른 방출 모두는 찾아가기에 어려울 수 있다. 따라서, 이러한 문제점을 극복하기 위해 디지털 콘텐츠를 특정적으로 찾아가는 방법 및 시스템이 필요하다.

디지털 콘텐츠의 보안을 위한 환경에 대한 다른 정보가 하기의 3가지 자원으로부터 발견될 수 있다. 뉴저지주의 Florham Park에 소재한 AT & T Labs사의 Jack Lacy, James Snyder, David Maher에 의한 온라인 URL

<http://www.a2bmusic.com/about/papers/musicipp.htm>을 사용하는 "인터넷상의 음악 및 지적 재산권 보호 문제". 캘리포니아주 Sunnyvale에 소재하며 온라인 URL <http://www.intertrust.com/architecture/stc.html>을 사용하는 InterTrust Technologies Corp.사의 Olin Sibert, David Bernstein 및 David Van Wie에 의한 논문 "무선 정보 교류에서 콘텐츠 보호". 온라인 URL <http://cyptolope.ibm.com/white.htm>을 사용하는 IBM White Paper에 기재된 "암호작성 컨테이너 기술".

발명의 구성 및 작용

본 발명의 목적은, 상기 언급한 단점을 제거하고 콘텐츠 데이터의 사용을 트래킹하기 위한 시스템을 제공하는 것이다. 본 발명의 일 실시예는 사용자 장치상에서 디지털 콘텐츠의 사용을 추정하기 위한 시스템을 제공하는 것이다. 디지털 콘텐츠를 배포하는 콘텐츠 사이트는 컴퓨터 판독가능 매체를 통해 사용자에게 제공된다. 네트워크에 연결된 전자 스토어는 디지털 콘텐츠 데이터를 사용자에게 플레이시키기 위해 인가를 판매한다. 이 인가는 트랜잭션을 특징적으로 식별하기 위한 특정 트랜잭션 식별자를 포함하고, 트랜잭션 시에 적어도 하나의 아이템을 특징적으로 식별하기 위한 특정 아이템 식별자를 포함한다. 인가를 가진 콘텐츠 데이터를 네트워크로부터 수신하는 콘텐츠 플레이어는 인가를 가진 콘텐츠 데이터를 플레이시키기 위해 사용된다. 콘텐츠 플레이어는 콘텐츠 식별자, 트랜잭션 식별자 및 아이템 식별자의 수학적 결합을 바탕으로 구매 식별자를 생성한다.

콘텐츠들의 표가 본 실시예에서 독자가 다른 섹션들로 신속하게 움직이는데 도움을 주기 위하여 본 발명에 제공된다.

I. 보안 디지털 콘텐츠 전자 배포 시스템

A. 시스템 개요

1. 권리 관리
2. 미터링(Metering)

3. 개방 구조

B. 시스템 기능적 요소

1. 콘텐츠 제공자(들)
2. 전자 디지털 콘텐츠 스토어(들)
3. 중간 마켓 파트너들
4. 클리어링하우스(들)(clearinghouse(s))
5. 최종 사용자 장치(들)
6. 전송 기반 시설

C. 시스템 이용

II. 암호화 개념 및 보안 디지털 콘텐츠 전자 배포 시스템으로의 이들의 애플리케이션

- A. 대칭 알고리즘
- B. 공용 키 알고리즘
- C. 디지털 기호
- D. 디지털 증명서
- E. SC(들)의 그래픽적 표현으로의 안내
- F. 보안 컨테이너 암호화 예

III. 보안 디지털 콘텐츠 전자 배포 시스템 흐름

IV. 권리 관리 구조 모델

A. 구조 총 기능

B. 기능 분리 및 흐름

1. 콘텐츠 포매팅층

2. 콘텐츠 사용 제어층

3. 콘텐츠 식별층

4. 인가 제어층

C. 콘텐츠 배포 및 인가 제어

V. 보안 컨테이너 구성

A. 일반 구성

B. 권리 관리 언어 신택스(Syntax) 및 시맨틱스(Semantics)

C. 보안 컨테이너 흐름 및 처리의 개요

D. 메타 데이터 보안 컨테이너(620) 포맷

E. 오퍼(Offer) 보안 컨테이너(641) 포맷

F. 트랜잭션 보안 컨테이너(640) 포맷

G. 오더 보안 컨테이너(650) 포맷

H. 인가 보안 컨테이너(660) 포맷

I. 콘텐츠 보안 컨테이너 포맷

VI. 보안 컨테이너 패킹(packing) 및 언패킹(unpacking)

A. 개요

B. 자료의 빌(Bill of Materials; BOM) 부문

C. 키 설명부

VII. 클리어링하우스(들)

A. 개요

B. 권리 관리 처리

C. 국가 지정 파라미터

D. 감사 로그 및 추적

E. 결과의 보고

G. 재전송

VIII. 콘텐츠 제공자

A. 개요

B. 워크 플로우 관리자

1. 저작물 대기 활동/정보 처리

2. 새로운 콘텐츠 요구 처리

3. 자동 메타 데이터 취득 처리
4. 수동 메타 데이터 엔트리 처리
5. 사용 조건 처리
6. 감시 릴리즈(release) 처리
7. 메타 데이터 SC(들) 생성 처리
8. 워터마킹(Watermarking) 처리
9. 전처리 및 압축 처리
10. 콘텐츠 품질 제어 처리
11. 암호화 처리
12. 콘텐츠 SC(들) 생성 처리
13. 최종 품질 보증 처리
14. 콘텐츠 분산 처리
15. 워크 플로우 규칙

C. 메타 데이터 융합(Assimilation) 및 엔트리 툴

1. 자동 메타 데이터 취득 툴
2. 수동 메타 데이터 엔트리 툴
3. 사용 조건 툴
4. 메타 데이터 SC(들)의 부문

5. 감시 릴리즈 툴

D. 콘텐츠 처리 툴

1. 워터마킹 툴
2. 전처리 및 압축 툴
3. 콘텐츠 품질 제어 툴
4. 암호화 툴

E. 콘텐츠 SC(들) 생성 툴

F. 최종 품질 보증 툴

G. 콘텐츠 분산 툴

H. 콘텐츠 프로모션 웹 사이트

I. 콘텐츠 호스팅

1. 콘텐츠 호스팅 사이트
2. 보안 디지털 콘텐츠 전자 배포 시스템에 의해 제공된 콘텐츠 호스팅 사이트(들)(111)

IX. 전자 디지털 콘텐츠 스토어(들)

A. 개요 - 다중 전자 디지털 콘텐츠 스토어(들)를 위한 지원

B. 포인트 투 포인트(Point-to-point)전자 디지털 콘텐츠 배포 서비스

1. 통합 요건

2. 콘텐츠 취득 톨

3. 트랜잭션 처리 모듈

4. 통지 인터페이스 모듈

5. 회계 조정 톨

C. 방송 전자 디지털 콘텐츠 배포 서비스

X. 최종 사용자 장치(들)

A. 개요

B. 애플리케이션 설치

C. 보안 컨테이너 처리기

D. 플레이어 애플리케이션

1. 개요

2. 최종 사용자 인터페이스 성분

3. 카피/플레이 관리 성분

4. 해독(1505), 압축 해제(1506) 및 플레이백 성분

5. 데이터 관리(1502) 및 라이브러리 액세스 성분

6. 애플리케이션간 통신 성분

7. 다른 갖가지 성분

8. 포괄적 플레이어

I. 보안 디지털 콘텐츠 전자 배포 시스템

A. 시스템 개요

보안 디지털 콘텐츠 전자 배포 시스템에는, 최종 사용자, 즉 클라이언트 장치에 디지털 콘텐츠와 디지털 콘텐츠 관련 콘텐츠의 권리 관리 및 보안 전달을 위해 필요한 기술, 명세, 톨 및 소프트웨어를 망라한 기술적인 플랫폼이 있다. 최종 사용자 장치(들)로는 PCS, 셋톱 박스(set top box; IRD) 및 인터넷 장치들이 있다. 상기 장치들은 콘텐츠 소유자들에 의해 허가되면 외부 매체 또는 휴대용 고객 장치들에 콘텐츠를 카피할 수 있다. 용어 디지털 콘텐츠, 즉 간략히 콘텐츠는 사진, 영화, 비디오, 음악, 프로그램, 멀티미디어 및 게임을 포함한 디지털 포맷으로 저장된 정보 및 데이터로 불리운다.

기술적인 플랫폼은 어떻게 디지털 콘텐츠가 준비되고, 최종 사용자 장치(들)에 인가된 방송 기반 시설(예컨대, 케이블, 인터넷, 위성 및 무선) 및 포인트 투 포인트를 통해 안전하게 배포되며, 인증되지 않은 카피나 플레이로부터 보호되는지를 설명한다. 또한, 기술적 플랫폼의 구조는 워터마킹, 압축/인코딩, 암호화 및 다른 보안 알고리즘 같은 여러 가지 기술들이 시간의 경과와 함께 발전함에 따라 이들의 통합 및 이전을 가능하게 한다.

보안 디지털 콘텐츠 전자 배포 시스템의 기본 성분들은: (1)콘텐츠 소유자의 소유권 보호를 위한 권리 관리; (2)즉각적인 정확한 보상을 위한 트랜잭션 미터링; 및 (3)콘텐츠 제공자(들)가 콘텐츠를 작성하고, 소정의 표준 순응 플레이어에서 플레이백시키기 위해 다중 네트워크 기반 시설상에 그 보안 전달을 허용하는 개방적이며 적절히 문서화된 구조를 포함한다.

1. 권리 관리

보안 디지털 콘텐츠 전자 배포 시스템에서의 권리 관리는 시스템의 조작 성분들 사이에 배포된 기능 세트를 통해 실행된다. 그 주 기

능은: 콘텐츠가 보안 인가를 갖는 최종 사용자(들) 또는 인증된 중개자에 의해서만 로크 해제되도록 하는 인가 인증 및 제어; 및 카피의 허용된 수, 플레이의 수 및 인가가 유효한 시간 간격 또는 기간 같은 인가 또는 구입 조건에 따른 콘텐츠 사용의 실시 및 제어를 포함한다. 권리 관리의 부 기능은 해적 행위에 맞서기 위해 콘텐츠의 인증되지 않은 카피의 원본을 식별할 수 있는 수단을 제공하는 것이다.

인가 인증 및 제어는 클리어링하우스(들) 엔티티 및 보안 컨테이너(SC) 기술을 이용하여 실행된다. 클리어링하우스(들)는 중간 또는 최종 사용자(들)가 인가 트랜잭션의 성공적인 종료의 검증 후, 콘텐츠를 로크 해제할 수 있도록 함으로써 인가 인증을 제공한다. 보안 컨테이너는 시스템 성분들 사이에 암호화된 콘텐츠 및 정보를 배포하기 위해 이용된다. SC는 전자 정보 및 콘텐츠의 비인증된 인터셉션 또는 변형으로부터 보호하기 위하여 암호화, 디지털 기호 및 디지털 증명을 이용하는 콘텐츠 또는 정보의 암호화 캐리어이다. 또한, 디지털 콘텐츠의 무결성 및 인증 검증을 허용한다. 상기 권리 관리 기능은 전자 디지털 콘텐츠 배포 기반 시설이 보안적이거나 또는 신뢰적이지 않기 때문에 장점이 있다. 따라서, 웹과 인터넷 같은 네트워크 기반 시설상에서의 전송을 허용한다. 이것은 콘텐츠가 보안 컨테이너 및 그 저장 장치에서 암호화되며, 배포가 그 로크 해제 및 이용의 제어로부터 독립적이라는 사실에 기인한다. 암호키를 갖고 있는 사용자만이 암호화된 콘텐츠를 로크 해제할 수 있으며, 클리어링하우스(들)는 인증된 적절한 사용 요구에 대해서만 암호키를 릴리즈한다. 클리어링하우스(들)는 미확인 또는 비인증된 자들로부터의 거짓 요구, 또는 콘텐츠 소유자들에 의해 설정된 것과 같은 콘텐츠의 사용 조건에 따르지 않는 요구를 클리어하지 않는다. 또한, SC가 그 전송중에 간섭받으면, 클리어링하우스(들) 내의 소프트웨어는 SC 내의 콘텐츠가 훼손되거나 또는 위조되었다고 판단하여, 트랜잭션을 거부한다.

콘텐츠 사용의 제어는 최종 사용자 장치(들)상에서 실행되는 최종 사용자 플레이어 애플리케이션(195)을 통해 이루어진다. 애플리케이션은 플레이어백 및 보조 카피의 허용가능한 횟수를 규정한 콘텐츠의 카피시마다 디지털 코드를 부여한다. 디지털 워터마킹 기술은 디지털 코드를 생성하고, 이것을 다른 최종 사용자 플레이어 애플리케이션(195)으로부터 숨겨지도록 유지하며, 이것을 변경 시도에 저항하도록 하기 위해 이용된다. 다른 실시예에서, 디지털 코드는 단지 콘텐츠(113)와 연관된 사용 조건의 일부로 유지된다. 디지털 콘텐츠(113)가 순응 최종 사용자 장치(들)에서 액세스되면, 최종 사용자 플레이어 애플리케이션(195)은 사용 제한을 검색하기 위해 워터마크를 판독하고, 필요에 따라 워터마크를 갱신한다. 콘텐츠의 요구된 이용이 사용 조건에 맞지 않는다면, 예컨대 카피의 횟수가 모두 소모되었다면, 최종 사용자 장치(들)는 요구를 수행하지 않게 된다.

디지털 워터마킹은 또한 인증된 원본이나 콘텐츠의 인증되지 않은 카피를 식별하기 위한 수단을 제공한다. 콘텐츠 내의 초기 워터마크는 콘텐츠 소유자를 식별하고, 저작권 정보를 나열하고, 지리적인 배포 지역을 규정하며, 다른 정당한 정보를 부가하기 위해 콘텐츠 소유자에 의해 매입된다. 이차 워터마크는 콘텐츠 구매자(또는, 인가자) 및 최종 사용자 장치(들)를 식별하고, 구입 또는 인가 조건 및 일자를 지정하며, 소정의 다른 정당한 정보를 부가하기 위해 최종 사용자 장치(들)에서의 콘텐츠에 매입된다.

워터마크는 콘텐츠의 필수 부분이기 때문에, 이들은 카피가 인증되는가의 여부에 관계없이 카피에 실려간다. 따라서, 디지털 콘텐츠는 항상 콘텐츠가 어디에 존재하고, 또는 출처가 어디인지에 관계없이 그 소스와 그 허가된 이용에 대한 정보를 포함한다. 상기 정보는 콘텐츠의 불법적인 이용에 대처하기 위해 이용될 수 있다.

2. 미터링

그 권리 관리 기능의 일부로서, 클리어링하우스(들)는 모든 트랜잭션의 기록을 유지하는데, 여기서 키 교환은 클리어링하우스(들)를 통해 클리어된다. 상기 기록은 이용의 원 조건과 인가 인증의 미터링을 고려한다. 트랜잭션 기록은 트랜잭션 지불과 다른 이용의 전자적 조정을 촉진하기 위해 곧바로 또는 주기적인 체제로 콘텐츠 소유자 또는 콘텐츠 제공자(들), 소매상들 같은 응답가능한 자들에게 보고될 수 있다.

3. 개방 구조

보안 디지털 콘텐츠 전자 배포 시스템(시스템)은 콘텐츠 소유자들에 대한 권리 보호를 유지하면서 시장에서의 시스템의 폭넓은 실행 및 수용을 촉진하기 위하여 발행된 명세 및 인터페이스를 갖는 개방 구조를 갖는다. 시스템 구조의 융통성 및 개방성은 또한 여러 가지 기술들, 전송 기반 시설 및 장치들이 시장에 보급됨에 따라 시스템이 발전될 수 있도록 한다.

구조는 콘텐츠 및 그 포맷의 성질에 있어 개방적이다. 오디오, 프로그램, 멀티미디어, 비디오 또는 다른 타입의 콘텐츠의 배포가 이 구조에 의해 지원받는다. 콘텐츠는 디지털 음악을 위한 선형 PCM 같은 자연 포맷 또는 부가적인 처리, 즉 필터링, 압축 또는 프리/디-앰퍼시스 등과 같은 인코딩에 의해 취득된 포맷으로 될 수 있다. 구조는 여러 가지 암호화 및 워터마킹 기술에 개방적이다. 특정한 기술의 선택으로 다른 콘텐츠 타입 및 포맷을 수용할 수 있도록 하며, 이들이 발전함에 따라 새로운 기술을 도입 또는 채택하도록 할 수 있다. 이러한 융통성은 콘텐츠 제공자(들)로 하여금 선택할 수 있도록 하여, 보안 디지털 콘텐츠 전자 배포 시스템에서의 데이터 압축, 암호화 및 포맷팅을 위해 이들이 이용하는 기술을 발전시킨다.

구조는 또한 다른 배포 네트워크와 다른 모델들에 개방적이다. 구조는 저속 인터넷 접속 또는 고속 위성 및 케이블 네트워크상에서의 콘텐츠 배포를 지원하며, 포인트 투 포인트나 방송 모델로 이용될 수 있다. 또한, 구조는 최종 사용자 장치(들)에서의 기능이 저비용 고객 장치를 포함한 폭넓은 장치들상에서 실행될 수 있도록 디자인된다. 이러한 융통성은 콘텐츠 제공자(들) 및 소매상들이 다양한 서비스 제공을 통해 중간 또는 최종 사용자(들)에게 콘텐츠를 제공할 수 있도록 하며, 사용자가 콘텐츠를 구매 또는 인가와, 이것의 플레이어백, 및 이것을 여러 가지 순응 플레이어 장치에 기록할 수 있도록 한다.

B. 시스템 기능 소자

도 1로 다시 돌아가면, 본 발명에 따른 보안 디지털 콘텐츠 전자 배포 시스템(100)의 개요를 예시한 블록도가 도시된다. 보안 디지털 콘텐츠 전자 배포 시스템(100)은, 콘텐츠 제공자(들)(101) 또는 디지털 콘텐츠의 소유자, 전자 디지털 콘텐츠 스토어(들)(103), 중간

시장 파트너(도시되지 않음), 클리어링하우스(들)(105), 콘텐츠 호스팅 사이트(111), 전송 기반 시설(107) 및 최종 사용자 장치(들)(109)를 포함한 엔드 투 엔드 솔루션을 갖는 여러 가지 사업 요소들을 포함한다. 상기 사업 요소들 각각은 보안 디지털 콘텐츠 전자 배포 시스템(100)의 여러 가지 성분들을 이용한다. 이들이 특히 전자 콘텐츠(113) 배포에 적합함에 따라, 상기 사업 요소 및 시스템 성분의 높은 수준의 설명이 뒤따른다.

1. 콘텐츠 제공자(들)(101)

콘텐츠 제공자(들)(101) 또는 콘텐츠 소유자(들)는 또 다른 배포를 위하여 독립된 콘텐츠(113)를 패키징하기 위해 인증된 원 콘텐츠(113)의 소유자 및/또는 배포자이다. 콘텐츠 제공자(들)(101)는 그들의 권리를 직접 활용하거나, 또는 일반적으로 전자 상거래 수익과 관련된 콘텐츠 사용료 지불에 대한 대가로 전자 디지털 콘텐츠 스토어(들)(103) 또는 중간 시장 파트너(도시되지 않음)에게 콘텐츠(113)를 인가할 수 있다. 콘텐츠 제공자(들)의 예는, 소니, 타임-워너, MTV, IBM, 마이크로소프트, 터너, 폭스 등일 수 있다.

콘텐츠 제공자(들)(101)는 그들의 콘텐츠(113) 및 배포를 위해 관련된 데이터를 작성하기 위하여 보안 디지털 콘텐츠 전자 배포 시스템(100)의 요소로 제공된 툴을 이용한다. 워크 플로우 관리자 툴(154)은 처리될 콘텐츠(113)를 예정하고, 고 품질 보증을 위해 여러 가지 단계의 콘텐츠(113) 작성 및 패키징을 거쳐 진행됨에 따라 콘텐츠(113)를 추적한다. 용어 "메타 데이터"는 콘텐츠(113)와 관련된 데이터를 설명하기 위하여 본 문서 전반에 걸쳐 이용되며, 본 실시예에서는 콘텐츠(113) 자체를 포함하지 않는다. 일례로서, 곡에 대한 메타 데이터는 곡명이나 곡 평판일 수 있지만, 곡의 사운드 녹음은 아니다. 콘텐츠(113)는 사운드 녹음을 포함할 수 있다. 메타 데이터 융합 및 엔트리 툴(161)은 콘텐츠 제공자(들)의 데이터베이스(160)로부터 메타 데이터를 추출하거나 또는 콘텐츠 제공자(들)에 의해 미리 규정된 포맷(예컨대, CD 제목, 가수명, 곡명, CD 삽화 같은 콘텐츠(113) 정보)으로 공급된 데이터를 추출하며, 이것을 전자 배포를 위해 패키징하기 위해 이용된다. 메타 데이터 융합 및 엔트리 툴(161)은 또한 콘텐츠(113)의 사용 조건을 기입하기 위해 이용된다. 사용 조건에서의 데이터는 필수적인 것으로 여겨지는 사업 규칙, 도매 가격, 카피 제한 규칙을 포함할 수 있다. 워터마킹 툴은 콘텐츠 소유자, 처리 일자 및 다른 관련 데이터를 식별하는 콘텐츠(113) 내의 데이터를 숨기기 위해 이용된다. 콘텐츠(113)가 오디오인 실시예에서, 오디오 전처리 툴은 강약을 조정하고 및/또는 콘텐츠(113)를 이퀄라이즈하기 위해 이용되며, 압축 품질을 최적화시키기 위한 다른 오디오는 콘텐츠(113)를 소망하는 압축 레벨로 압축하고, 콘텐츠(113)를 암호화시킨다. 이것은 이들이 시장에서 발전함에 따라 콘텐츠 제공자(들)(101)가 최상의 툴을 이용할 수 있도록 하여, 디지털 콘텐츠 압축/인코딩, 암호화 및 포맷팅에서의 기술적 진보에 맞춰 적용될 수 있다.

암호화된 콘텐츠(113), 디지털 콘텐츠 관련 데이터 또는 메타 데이터 및 암호화된 키는 SC 패커(packer) 툴에 의해 SC들(이하에 설명됨)로 팩되고, 전자 배포를 위한 콘텐츠 호스팅 사이트 및/또는 프로모션형 웹 사이트에 저장된다. 콘텐츠 호스팅 사이트는 전자 디지털 콘텐츠 스토어(들)(103) 및 중간 시장 파트너(도시되지 않음) 설비를 갖는 다중 장소 또는 콘텐츠 제공자(들)(101)에 있을 수 있다. 콘텐츠(113) 및 키(이하에 설명됨)는 모두 암호화되어 SC들로 팩되기 때문에, 전자 디지털 콘텐츠 스토어(들)(103) 또는 소정의 다른 호스팅 에이전트는 클리어링하우스(들)로부터의 클리어링과 콘텐츠 제공자(들)(101)로의 통지없이 암호화된 콘텐츠(113)에 직접 액세스할 수 없다.

2. 전자 디지털 콘텐츠 스토어(들)(103)

전자 디지털 콘텐츠 스토어(들)(103)는 콘텐츠(113) 테마 프로그래밍 또는 콘텐츠(113)의 전자 거래 같은 매우 다양한 서비스 또는 애플리케이션을 통해 콘텐츠(113)를 마켓하는 엔티티이다. 전자 디지털 콘텐츠 스토어(들)(103)는 디자인, 개발, 사업 경영, 청구, 거래, 마케팅 및 이러한 서비스의 판매 활동을 관리한다. 예시적 온라인 전자 디지털 콘텐츠 스토어(들)(103)는 소프트웨어의 전자 다운로드를 제공하는 웹 사이트이다.

이러한 서비스들에서, 전자 디지털 콘텐츠 스토어(들)(103)는 보안 디지털 전자 배포 시스템(100)의 소정의 기능을 실행한다. 전자 디지털 콘텐츠 스토어(들)(103)는 부가적 SC들 내의 메타 데이터, 팩 콘텐츠 및 콘텐츠 제공자(들)(101)로부터의 정보를 수집하고, 상기 SC들을 고객 또는 거래처에게 서비스 또는 애플리케이션의 일부로서 전달한다. 전자 디지털 콘텐츠 스토어(들)(103)는 메타 데이터 추출, 이차 처리 조건, SC 패키징 및 전자 콘텐츠 트랜잭션의 추적을 돕기 위하여 보안 디지털 콘텐츠 전자 배포 시스템(100)에 의해 제공된 툴을 이용한다. 이차 처리 조건 데이터는 시간적 가용성 제한 또는 콘텐츠(113) 구입 가격, 페이-퍼-리슨(pay-per-listen) 가격, 카피 인증 및 타겟 장치 형태 같은 소매 사업 제한을 포함할 수 있다.

전자 디지털 콘텐츠 스토어(들)(103)가 최종 사용자(들)로부터 전자 콘텐츠(113)에 대한 유효한 요구를 갖추면, 전자 디지털 콘텐츠 스토어(들)(103)는 고객에게 콘텐츠(113)에 대한 해독화 키를 릴리즈하기 위하여 클리어링하우스(들)를 인증해야 한다. 전자 디지털 콘텐츠 스토어(들)는 또한 콘텐츠(113)를 포함한 SC(들)의 다운로드를 인증한다. 전자 디지털 콘텐츠 스토어(들)는 그 로컬 사이트에서 디지털 콘텐츠를 갖는 SC들을 호스팅하기 위한 선택을 하고, 및/또는 다른 콘텐츠 호스팅 사이트의 호스팅 및 배포 설비를 활용할 수 있다.

전자 디지털 콘텐츠 스토어(들)는 최종 사용자(들)가 보안 디지털 콘텐츠 전자 배포 시스템(100)을 이용할 때 갖을 수 있는 소정의 질문 또는 문제에 대한 고객 서비스를 제공하거나, 전자 디지털 콘텐츠 스토어(들)(103)는 클리어링하우스(들)(105)와 그들의 고객 서비스 지원에 대한 계약을 할 수 있다.

3. 중간 마켓 파트너(도시되지 않음)

다른 실시예에서, 보안 디지털 콘텐츠 전자 배포 시스템(100)은 콘텐츠(113)를 중간 마켓 파트너로 불리우는 다른 사업자에게 안전하게 제공하기 위해 이용될 수 있다. 상기 파트너는 콘텐츠(113)를 배포하는 텔레비전국 또는 비디오 클럽, 라디오국 또는 녹음 클럽 같은 비-전자 서비스를 제공하는 디지털 콘텐츠-관련 회사를 포함할 수 있다. 상기 파트너는 또한 녹음 스튜디오, 복제자 및 생산자 같은 제작 또는 마케팅 사운드 녹음의 일부로서 관리하는 다른 신뢰받는 대상을 포함할 수 있다. 상기 중간 마켓 파트너들은 콘텐츠

(113)를 해독하기 위하여 클리어링하우스(들)(105)로부터의 클리어링을 필요로 한다.

4. 클리어링하우스(들)(105)

클리어링하우스(들)(105)는 SC에 암호화된 콘텐츠(113)의 허용된 이용 및/또는 판매 활동과 관련된 모든 트랜잭션을 유지하는 기록 및 인가 인증을 제공한다. 클리어링하우스(들)(105)가 중간 또는 최종 사용자(들)로부터 콘텐츠(113)에 대한 해독키 요구를 수신하면, 클리어링하우스(들)(105)는 요구에서의 정보의 인증 및 무결점을 확인하고, 요구가 전자 디지털 콘텐츠 스토어(들) 또는 콘텐츠 제공자(들)(101)에 의해 인증되었는가를 검증하며, 요구된 사용이 콘텐츠 제공자(들)(101)에 의해 규정된 바와 같은 콘텐츠 사용 조건을 따르는가를 검증한다. 상기 검증이 충족되면, 클리어링하우스(들)(105)는 콘텐츠(113)에 대한 해독키를 인가 SC에 팩된 요구 최종 사용자(들)에게 전송한다. 키는 인증된 사용자만이 이것을 검색할 수 있도록 하는 방식으로 암호화된다. 만약, 최종 사용자의 요구가 검증될 수 없거나, 완전하지 않거나 또는 인증되지 않았다면, 클리어링하우스(들)(105)는 해독키에 대한 요구를 거부한다.

클리어링하우스(들)(105)는 모든 트랜잭션의 기록을 유지하고, 이들을 중간에, 주기적으로 또는 제한적으로 전자 디지털 콘텐츠 스토어(들)(103) 및 콘텐츠 제공자(들)(101) 같은 신뢰할 수 있는 대상에게 통보한다. 이러한 통보는 콘텐츠 제공자(들)(101)가 콘텐츠(113)의 판매를 통지할 수 있고, 전자 디지털 콘텐츠 스토어(들)(103)가 그들의 고객으로의 전자 전달의 회계 자료를 얻을 수 있도록 하는 수단이다. 클리어링하우스(들)(105)는 또한 SC 내의 정보가 손상되거나 또는 콘텐츠의 사용 조건에 따르지 않음을 발견하면, 콘텐츠 제공자(들)(101) 및 전자 디지털 콘텐츠 스토어(들)(103)에 통지할 수 있다. 클리어링하우스(들)(105) 데이터베이스의 트랜잭션 기록 및 보관 자격은 데이터 마이닝(mining) 및 보고 발생을 위해 구성된다.

다른 실시예에서, 클리어링하우스(105)는 반품, 전송 실패 및 구매 논쟁 같은 트랜잭션을 위한 고객 지원 및 불만 처리를 제공할 수 있다. 클리어링하우스(들)(105)는 권리 관리 및 미터링(metering)을 위한 신뢰있는 관리자를 제공하여 독립적인 엔티티로서 동작될 수 있다. 필요에 따라서는 빌링(billing) 및 결제를 제공한다. 전자 클리어링하우스(들)의 예로 비자/마스터카드로부터의 보안 전자 트랜잭션(SET) 및 Secure-Bank.com이 있다. 일 실시예에서, 클리어링하우스(들)(105)는 최종 사용자 장치(들)(109)에 액세스가능한 웹 사이트이다. 다른 실시예에서, 클리어링하우스(들)(105)는 전자 디지털 콘텐츠 스토어(들)(103)의 일부이다.

5. 최종 사용자 장치(들)(109)

최종 사용자 장치(들)(109)는 보안 디지털 콘텐츠 전자 배포 시스템(100) 명세에 따르는 최종 사용자 플레이어 애플리케이션(195; 이후에 설명됨)을 포함한 소정의 플레이어 장치일 수 있다. 상기 장치들은 PCS, 셋톱 박스들(IRD들) 및 인터넷 장치를 포함할 수 있다. 최종 사용자 플레이어 애플리케이션(195)은 소프트웨어 및/또는 고객 전자 하드웨어로 실행될 수 있다. 플레이, 기록 및 라이브러리 관리 기능을 수행함과 더불어, 최종 사용자 플레이어 애플리케이션(195)은 최종 사용자 장치(들)(109)에서의 권리 관리를 할 수 있도록 SC 처리를 수행한다. 최종 사용자 장치(들)(109)는 디지털 콘텐츠를 갖는 SC들의 저장 및 다운로드를 관리하고, 클리어링하우스(들)(105)로부터 암호화된 디지털 콘텐츠 키의 수신을 관리하고, 디지털 콘텐츠가 카피되거나 또는 플레이될 때마다 워터마크(들)를 처리하고, 디지털 콘텐츠의 사용 조건에 따라 이루어진 카피의 횟수(또는, 카피 삭제의 횟수)를 관리하며, 허용된다면 외부 매체 또는 휴대용 고객 장치에 카피를 수행한다. 휴대용 고객 장치는 워터마크에 매입된 콘텐츠의 사용 조건을 처리하기 위하여 최종 사용자 플레이어 애플리케이션(195)의 일부를 수행할 수 있다. 용어 "최종 사용자(들)" 및 "최종 사용자 플레이어 애플리케이션(195)"은 최종 사용자 장치(들)(109)에서의 전반적인 이용 또는 운영을 의미하는 것으로 사용된다.

6. 전송 기반 시설(107)

보안 디지털 콘텐츠 전자 배포 시스템(100)은 전자 디지털 콘텐츠 스토어(들)(103)와 최종 사용자 장치(들)(109)를 접속시키는 전송 망과는 독립적이며, 인터넷 같은 포인트 투 포인트와 디지털 방송 텔레비전 같은 방송 배포 모델을 모두 지원할 수 있다.

동일한 톨 및 애플리케이션이 여러 가지 전송 기반 시설(107)상에서 콘텐츠(113) 트랜잭션을 얻고, 패키징하며 추적하기 위해 이용되더라도, 서비스가 고객에게 전달되는 방법 및 표현은 기반 시설 및 선택된 배포 모델에 따라 변화될 수 있다. 높은 대역폭의 기반 시설이 낮은 대역폭의 기반 시설 보다 더 적절한 응답 시간으로 높은 품질의 디지털 콘텐츠를 전달할 수 있기 때문에, 전송되는 콘텐츠의 품질이 또한 변화될 수 있다. 포인트 투 포인트 배포 모델로 디자인된 서비스 애플리케이션은 또한 방송 배포 모델을 지원하기 위해 적응될 수 있다.

C. 시스템 사용

보안 디지털 콘텐츠 전자 배포 시스템(100)은 고품질의 보안 전달, 고객 또는 사업자의 최종 사용자 장치(들)(109)로의 콘텐츠(113)의 전자 카피를 가능하게 하며, 콘텐츠(113) 사용의 표준화 및 추적을 가능하게 한다.

보안 디지털 콘텐츠 전자 배포 시스템(100)은 새로운 것과 기존의 배포 채널을 모두 이용하여 다양한 고객들 및 사업자 대 사업자 서비스로 전개될 수 있다. 각 특정한 서비스는 보안 디지털 콘텐츠 전자 배포 시스템(100)의 권리 관리 특징을 통해 제공될 수 있는 다른 금융 모델을 이용할 수 있다. 도매 또는 소매 구입, 페이-퍼-리슨 사용, 가입자 서비스, 카피/카피 거부 제한 또는 재배포 같은 모델들은 클리어링하우스(들)(105)의 권리 관리 및 최종 사용자 플레이어 애플리케이션(195) 카피 방지 특징을 통해 실행될 수 있다.

보안 디지털 콘텐츠 전자 배포 시스템(100)은 콘텐츠(113)를 판매 서비스의 발생시 전자 디지털 콘텐츠 스토어(들)(103) 및 중간 마켓 파트너에게 큰 융통성을 허용한다. 동시에, 디지털 자산이 보호되고 미터링되는 보증 레벨을 갖는 콘텐츠 제공자(들)(101)를 제공하여, 이들이 콘텐츠(113)의 인가를 위한 적절한 보상을 받을 수 있도록 한다.

II. 암호화 개념 및 보안 디지털 콘텐츠 전자 배포 시스템으로의 이들의 애플리케이션

A. 대칭 알고리즘

보안 디지털 콘텐츠 전자 배포 시스템(100)에서, 콘텐츠 제공자(들)(101)는 대칭적 알고리즘을 이용하여 콘텐츠를 암호화한다. 이들은 동일한 키가 데이터를 암호화 및 해독화를 위해 이용되기 때문에, 대칭적 알고리즘으로 불리운다. 데이터 전송자 및 메시지 수신자는 키를 공유해야 한다. 공유된 키는 본 명세서에서 대칭 키로 불리운다. 보안 디지털 콘텐츠 전자 배포 시스템(100) 구조는 특정한 실행을 위해 선택된 특정 대칭 알고리즘과는 독립적이다.

일반적인 대칭 알고리즘으로는 DES, RC2 및 RC4가 있다. DES 및 RC2는 블록 암호화기이다. 블록 암호화기는 데이터 비트의 블록을 이용해 한꺼번에 데이터를 암호화한다. DES는 공무상의 US 정부 암호화 표준이며, 64 비트 블록 크기를 갖고, 56 비트 키를 이용한다. 트리플-DES는 일반적으로 단순 DES로 구현되는 보안을 높이기 위해 이용된다. RAS 데이터 보안으로 RC2를 디자인한다. RC2는 가변키 크기 암호화기를 이용하여, 64 비트의 블록 크기를 갖는다. RC4는 또한 RSA 데이터 보안에 의해 디자인되며, 가변키 크기 스트림 암호화기이다. 스트림 암호화기는 단일 데이터 비트를 한꺼번에 동작시킨다. RAS 데이터 보안은 RC4에 출력 바이트마다 8개 내지 16개의 기기 연산이 필요함을 요구한다.

IBM은 SEAL로 불리우는 고속 알고리즘을 디자인한다. SEAL은 가변 길이 키를 이용하여 32 비트 처리기용으로 최적화된 스트림 알고리즘이다. SEAL은 데이터 바이트마다 대략 5개 정도의 기본 기기 명령을 필요로 한다. 50MHZ, 486 기반의 컴퓨터는, 이용되는 160 비트 키가 이미 내부 표로 전처리되었다면, 7.2메가바이트/초로 SEAL 코드를 운영한다.

마이크로소프트는 암호화 API 문서의 개요에서의 암호화 성능 벤치마크의 결과를 보고한다. 이 결과는 윈도우 NT 4.0을 갖는 120MHZ 펜티엄 기반 컴퓨터상에서 운영되는 마이크로소프트사의 암호화 API를 이용하는 애플리케이션에 의해 구해진다.

암호화기	키 크기	키 셋업 시간	암호화 속도
DES	56	460	1,138,519
RC2	40	40	286,888
RC4	40	151	2,377,723

B. 공용 키 알고리즘

보안 디지털 콘텐츠 전자 배포 시스템(100)에서, 대칭 키 및 다른 작은 데이터 피스는 공용 키를 이용하여 암호화된다. 공용 키 알고리즘은 2개의 키를 이용한다. 이 2개의 키는 한 키로 암호화된 데이터가 다른 키로 해독될 수 있도록 수학적으로 관련된다. 키의 소유자들은 하나의 키를 개인적인 것(개인 키)으로 보존하며, 공개적으로 제 2 키(공용 키)를 배포한다.

공용 키 알고리즘을 이용하여 비밀 메시지의 전송을 보안하기 위하여, 메시지를 암호화하기 위한 수신인의 공용 키를 이용해야 한다. 연관된 개인 키를 갖는 수신인만이 메시지를 해독할 수 있다. 공용 키 알고리즘은 또한 디지털 기호를 생성하기 위해 이용된다. 개인 키는 상기 목적을 위해 이용된다. 다음의 섹션은 디지털 기호에 관한 정보를 제공한다.

가장 일반적으로 이용되는 공용 키 알고리즘으로는 RSA 공용 키 암호화기가 있으며, 이것은 사실상 산업에서의 공용 키 표준으로 되었다. 또한, 암호화를 위해 작업되는 다른 알고리즘과 디지털 기호로는 ElGamal 및 Rabin이 있다. RSA는 가변 키 길이 암호화기이다.

대칭 키 알고리즘은 공용 키 알고리즘 보다 훨씬 빠르다. 소프트웨어에서, DES는 일반적으로 RSA 와 같이 적어도 100배 빠르다. 이 때문에, RSA는 대량의 데이터를 암호화하기 위해 이용되지 않는다. RSA 데이터 보안은 90MHZ 펜티엄 기기상에서 RSA 데이터 보안의 툴 키트 BSAFE 3.0이 512 비트율로 21.6 킬로비트/초, 및 1024 비트율로 7.4 킬로비트/초의 개인 키 동작(개인 키를 이용한 암호화 또는 해독화)에 대한 처리율을 갖음을 보고한다.

C. 디지털 기호

보안 디지털 콘텐츠 전자 배포 시스템(100)에서, SC(들)의 발행인은 이것을 디지털적으로 부호화함으로써 SC(들)의 무결성을 보호한다. 일반적으로, 메시지의 디지털 기호를 만들기 위하여, 메시지 소유자는 우선 메시지 다이제스트(digest)를 계산하고(이하에 설명됨), 소유자의 개인 키를 이용하여 메시지 다이제스트를 암호화한다. 메시지는 그 기호로 배포된다. 메시지의 소정의 수신인은 메시지 다이제스트를 회복하기 위해 메시지 소유자의 공용 키를 이용하여 우선 기호를 해독함으로써 디지털 기호를 검증할 수 있다. 이때, 수신인은 수신된 메시지의 다이제스트를 계산하고, 이것을 회복된 것과 비교한다. 만약, 메시지가 배포중에 변경되지 않았다면, 계산된 다이제스트와 회복된 다이제스트는 동일해야 한다.

보안 디지털 콘텐츠 전자 배포 시스템(100)에서, SC(들)는 여러 개의 데이터부문들을 포함하기 때문에, 다이제스트는 각 부문마다 계산되고, 요약 다이제스트는 연결된 부문 다이제스트마다 계산된다. 요약 다이제스트는 SC(들) 발행인의 개인 키를 이용하여 암호화된다. 암호화된 요약 다이제스트는 SC(들)에 대한 발행인의 디지털 기호이다. 부문 다이제스트 및 디지털 기호는 SC(들)의 본문에 포함된다. SC(들)의 수신인은 수신된 디지털 기호 및 부문 다이제스트에 의해 SC(들)와 그 부문의 무결성을 검증할 수 있다.

한 방향의 해시(hash) 알고리즘이 메시지 다이제스트를 계산하기 위해 이용된다. 해시 알고리즘은 가변 길이 입력 메시지를 취하고, 이것을 고정 길이 스트림 메시지 다이제스트로 변환한다. 한 방향 해시 알고리즘은 한 방향으로만 동작한다. 즉, 입력 메시지에 대한 다이제스트를 계산하는 것은 쉽지만, 그 다이제스트로부터 입력 메시지를 발생시키는 것은 매우 어렵다. 한 방향 해시 기능의 특성 때

문에, 사람들은 메시지 다이제스트를 메시지의 지문으로 생각한다.

더 일반적인 한 방향 해시 기능으로는 미국 기술 및 표준 국가 협회(NITS)에 의해 디자인된 SHA 및 RSA 데이터 보안으로부터의 MD5가 있다.

D. 디지털 증명서

디지털 증명서는 디지털적으로 부호화된 메시지를 전송한 사람 또는 엔티티의 동일성을 인증 또는 증명하기 위해 이용된다. 증명서는 공용 키와 사람 또는 엔티티를 결속하는 증명 기관에 의해 발행된 디지털 문서이다. 증명서는 공용 키, 사람 또는 엔티티의 이름, 만료일, 증명 기관의 이름 및 다른 정보를 포함한다. 증명서는 또한 증명 기관의 디지털 기호를 포함한다.

엔티티(또는, 사람)가 그 개인 키로 부호화되고 그 디지털 증명서가 동반된 메시지를 전송하면, 메시지의 수신인은 메시지를 수령하는가의 여부를 결정하기 위하여 증명서로부터 엔티티의 이름을 이용한다.

보안 디지털 콘텐츠 전자 배포 시스템(100)에서, 최종 사용자 장치(들)(109)에 의해 발행된 것 이외의 모든 SC(들)는 SC(들) 제작자의 증명서를 포함한다. 많은 최종 사용자(들)가 증명서 취득을 꺼려하지 않거나, 또는 진정하지 않은 증명 기관에 의해 발행된 증명서를 갖을 수 있기 때문에, 최종 사용자 장치(들)(109)는 그들의 SC(들)의 증명서를 포함할 필요가 없다. 보안 디지털 콘텐츠 전자 배포 시스템(100)에서, 클리어링하우스(들)(105)는 전자 디지털 콘텐츠 스토어(들)(103)로의 증명서 발행을 위한 옵션을 갖는다. 이로서, 최종 사용자 장치(들)(109)는 전자 디지털 콘텐츠 스토어(들)(103)가 보안 디지털 콘텐츠 전자 배포 시스템(100)에 의해 인증되었음을 독립적으로 검증할 수 있다.

E. SC(들)의 그래픽적 표현으로의 안내

본 문서는 암호화된 부분, 비-암호화된 부분, 암호화 키 및 증명서를 보여주는 SC(들)를 그래픽적으로 표현하기 위해 도면을 이용한다. 이제부터 SC(들)(200)의 예시적 도면인 도 2를 참조한다. 다음의 심볼들은 SC(들) 도면에 이용된다. 키(201)는 공용 또는 개인 키이다. 키의 이(teeth), 예컨대 클리어링하우스용 CLRNGH는 키 소유주를 나타낸다. 조종부 내의 PB는 이것이 공용 키임을 나타내고, 따라서 키(201)는 클리어링하우스 공용 키이다. 조종부 내의 PV는 이것이 개인 키임을 나타낸다. 다이아몬드 형상은 최종 사용자(들)의 디지털 기호(202)이다. 이니셜은 개인 키가 기호를 생성하기 위해 이용됨을 나타내고, 따라서 EU는 이하의 표에서는 최종 사용자(들)의 디지털 기호이다. 대칭 키(203)는 콘텐츠를 암호화하기 위해 이용된다. 암호화된 대칭 키 객체(204)는 CLRNGH의 PB로 암호화된 대칭 키(203)를 포함한다. 직사각형의 상부 테두리상의 키는 객체의 암호화에 이용된 키이다. 직사각형 내의 심볼 또는 문자는 암호화된 객체(이 경우에는 대칭 키)를 나타낸다. 다른 암호화된 객체로, 본 예에서는 트랜잭션 ID 암호화 객체(205)가 도시된다. 그리고, 사용 조건(206), 트랜잭션 ID 암호화 객체(207) 및 암호화된 대칭 키 객체(204)는 모두 최종 사용자 디지털 기호(202)로 부호화된다.

이하의 표는 SC(들)의 부호를 식별하는 이니셜을 도시한다.

이니셜	성분
CP	콘텐츠 제공자(들)(101)
MS	전자 디지털 콘텐츠 스토어(들)(103)
HS	콘텐츠 호스팅 사이트(들)(111)
EU	최종 사용자 장치(들)(109)
CH	클리어링하우스(들)(105)
CA	증명 기관(들)(도시되지 않음)

F. 보안 컨테이너 암호화 예

이하의 표 및 도면은 SC(들)로부터 정보를 생성하고 회복하기 위해 이용되는 암호화 및 해독화 처리의 개요를 제공한다. 상기 처리 개요에서, 생성 및 해독화된 SC(들)는 일반적인 SC(들)이다. 보안 디지털 콘텐츠 전자 배포 시스템(100)에서 권리 관리를 위해 이용되는 특정한 SC(들) 타입은 전혀 나타나지 않았다. 처리는 암호화 처리를 위해 도 3에 설명된 스텝들로 구성된다.

도 3의 암호화 처리를 위한 처리 흐름스텝 처리301 송신자는 랜덤한 대칭 키를 생성하고, 콘텐츠를 암호화하기 위하여 이것을 이용한다.

302 송신자는 콘텐츠 다이제스트를 생성하기 위하여 해시 알고리즘을 통해 암호화된 콘텐츠를 실행한다.

303 송신자는 수신자의 공용 키를 이용하여 대칭 키를 암호화한다. PB RECPNT는 수신자의 공용 키를 말한다.

304 송신자는 대칭 키 다이제스트를 만들기 위하여 스텝 2에서 이용된 것과 동일한 알고리즘을 통해 암호화된 대칭 키를 실행한다.

305 송신자는 SC(들) 다이제스트를 만들기 위해 스텝 2에서 이용된 것과 동일한 해시 알고리즘을 통해 콘텐츠 다이제스트와 대칭 키 다이제스트의 연결을 실행한다.

306 송신자는 SC(들)에 대한 디지털 기호를 만들기 위해 송신자의 개인 키로 SC(들) 다이제스트를 암호화한다. PV SENDER는 전송 자워 개인 키를 말한다.

307B 송신자는 암호화된 콘텐츠, 암호화된 대칭 키, 콘텐츠 다이제스트, 대칭 키 다이제스트, 송신자의 증명서 및 SC(들) 기호를 포함한 SC(들) 파일을 생성한다.

307A 송신자는 보안 통신을 개시하기 전에 증명 기관으로부터 증명서를 취득해야만 한다. 증명 기관은 증명서에 송신자의 공용 키, 송신자의 이름을 포함하고, 이것을 부호화한다. PV CAUTHR은 증명 기관의 개인 키를 말한다.

도 4의 암호화 처리를 위한 처리 흐름스텝 처리408 수신자는 SC(들)을 수신하고, 그 부문들을 분리한다.

409 수신자는 송신자의 증명서 내의 디지털 기호를 증명 기관의 공용 키로 해독함으로써 검증한다. 만약, 증명서의 디지털 기호가 정당한 것이라면, 수신자는 증명서로부터 송신자의 공용 키를 취득한다.

410 수신자는 송신자의 공용 키를 이용하여 SC(들) 디지털 기호를 해독한다. 이로서 SC(들) 다이제스트를 회복한다. PB SENDER는 송신자의 공용 키를 말한다.

411 수신자는 SC(들) 다이제스트를 계산하기 위하여 송신자에 의해 이용된 것과 동일한 해시 알고리즘을 통해 수신된 콘텐츠 다이제스트와 암호화된 키 다이제스트의 연결을 실행한다.

412 수신자는 계산된 SC(들) 다이제스트를 송신자의 디지털 기호로부터 회복된 것과 비교한다. 만약, 이들이 동일하다면, 수신자는 수신된 다이제스트가 변경되지 않았음을 확인하고, 해독화 처리를 지속한다. 만약, 이들이 동일하지 않다면, 수신자는 SC(들)를 버리고 전송자에게 통보한다.

413 수신자는 대칭 키 다이제스트를 계산하기 위하여 스텝 411에서 이용된 것과 동일한 해시 알고리즘을 통해 암호화된 대칭 키를 실행한다.

414 수신자는 계산된 대칭 키 다이제스트와 SC(들)에서 수신된 것을 비교한다. 만약, 이들이 동일하다면, 수신자는 암호화된 대칭 키가 변경되지 않았음을 알 수 있다. 수신자는 해독화 처리를 지속한다. 만약, 정당한 것이 아니라면, 수신자는 SC(들)를 버리고 전송자에게 통보한다.

415 수신자는 콘텐츠 다이제스트를 계산하기 위하여 스텝 411에서 이용된 것과 동일한 해시 알고리즘을 통해 암호화된 콘텐츠를 실행한다.

416 수신자는 계산된 콘텐츠 다이제스트와 SC(들)에서 수신된 것을 비교한다. 만약, 이들이 동일하다면, 수신자는 암호화된 콘텐츠가 변경되지 않았음을 알 수 있다. 이때, 수신자는 해독화 처리를 지속한다. 만약, 정당한 것이 아니라면, 수신자는 SC(들)를 버리고 송신자에게 통보한다.

417 수신자는 수신자의 개인 키를 이용하여 암호화된 대칭 키를 해독한다. PV RECPNT는 수신자의 개인 키를 말한다.

418 수신자는 암호화된 콘텐츠를 해독하기 위하여 대칭 키를 이용한다. 이로서 콘텐츠를 회복한다.

III. 보안 디지털 콘텐츠 전자 배포 시스템 흐름

보안 전자 디지털 콘텐츠 배포 시스템(100)은 시스템의 다른 참여자에 의해 이용되는 여러 가지 성분들로 구성된다. 상기 참여자는 콘텐츠 제공자(들)(101), 전자 디지털 콘텐츠 스토어(들)(103), 최종 사용자 장치(들)(109)를 통과하는 최종 사용자(들) 및 클리어링 하우스(들)(105)를 포함한다. 고레벨 시스템 흐름은 보안 디지털 콘텐츠 전자 배포 시스템(100)의 개요에 따라 이용된다. 하기에 개요가 설명되는 상기 흐름은 시스템(100)을 전체적으로 흐름에 따라 콘텐츠를 추적한다. 또한, 구입, 로크 해제 및 콘텐츠(113)의 이용을 위한 트랜잭션을 수행하기 위해 참가자에 의해 이용되는 스텝들의 개요가 설명된다.

- 이것은 디지털 콘텐츠 서비스(PC와의 포인트 투 포인트 인터페이스)를 위한 시스템 흐름이다.
- 콘텐츠 제공자(들)(101)는 (음악 오디오 예로서)PCM 비압축된 포맷으로 오디오 디지털 콘텐츠를 제공한다.
- 콘텐츠 제공자(들)(101)는 ODBC 순응 데이터베이스 내의 메타 데이터를 갖거나, 또는 콘텐츠 제공자(들)(101)는 데이터를 직접 콘텐츠 정보 처리 보조 시스템에 기입하거나 또는 규정된 ASC II 파일 포맷(들)으로 데이터를 공급할 수 있다.
- 금융 결제는 전자 디지털 콘텐츠 스토어(들)에 의해 수행된다.
- 콘텐츠(113)는 단일 콘텐츠 호스팅 사이트(들)(111)에서 호스트된다.

상기한 가정들이 예컨대 음악, 비디오와 프로그램 및 전자 배포 시스템 방송 같은 디지털 콘텐츠의 엄격한 성질을 수용하기 위해 변경될 수 있음을 당 기술에 숙련된 지식을 가진 자들은 이해할 수 있을 것이다.

도 1에 예시된 것 다음의 처리 흐름스텝 처리121 비압축된 PCM 오디오 파일은 콘텐츠 제공자(들)(101)에 의해 콘텐츠(113)로서 공급된다. 그 파일명은 콘텐츠(113)에 대한 콘텐츠 제공자(들)(101)의 유일 식별자와 함께 워크 플로우 관리자(154)에 입력된다.

122 메타데이터는 맵핑 템플릿에 의해 제공된 정보와 콘텐츠(113)에 대한 콘텐츠 제공자(들)(101)의 유일 식별자를 이용하여 콘텐츠 정보 처리 보조 시스템에 의해 콘텐츠 제공자(들)의 데이터베이스(160)로부터 입수된다.

123 워크 플로우 관리자 툴(154)은 콘텐츠 제공자(들)(101)에서 취득 및 작성 처리를 통해 콘텐츠 흐름을 지시하기 위해 이용된다. 이것은 또한 항상 시스템에서의 소정 피스의 콘텐츠의 상태를 추적하기 위해 이용된다.

124 콘텐츠(113)에 대한 사용 조건은 콘텐츠 정보 처리 보조 시스템에 기입되며, 이것은 수동으로 또는 자동으로 수행될 수 있다. 이 데이터는 카피 제한 규칙 및 필수적인 것으로 여겨지는 소정의 다른 규칙을 포함한다. 메타 데이터 엔트리 모두는 데이터에 대한 오디오 처리와 병행하여 발생할 수 있다.

125 워터마킹 툴은 콘텐츠 제공자(들)(101)가 콘텐츠를 식별하기 위해 필수적인 것으로 여겨지는 콘텐츠(113) 내의 데이터를 숨기기 위해 이용된다. 이것은 언제 입수되었는가, 어디서 발생한 것인가(상기 콘텐츠 제공자(들)(101)로부터 발생한 것인가), 또는 어떠한 다른 정보가 콘텐츠 제공자(들)(101)에 의해 지정되는 가를 포함할 수 있다.

- 콘텐츠 처리 툴(125)은 지원되는 다른 압축에서 필요한 것과 같이, 콘텐츠(113)에 등화, 동적 조정 및 재생플링을 수행한다.

- 콘텐츠(113)는 콘텐츠 처리 툴(125)을 이용하여 소망하는 압축 레벨로 압축된다. 이후, 콘텐츠(113)는 압축이 소망하는 레벨로 콘텐츠(113) 품질을 생성하는 가를 검증하기 위하여 플레이백 될 수 있다. 필요하다면, 등화, 동적 조정, 압축 및 플레이백 품질 검색이 소망하는 횟수만큼 수행될 수 있다.

- 콘텐츠(113) 및 그 메타 데이터의 서브셋은 SC 패커에 의해 대칭 키로 암호화된다. 이후, 상기 툴은 암호화된 대칭 키를 생성하기 위하여 클리어링하우스(들)(105)의 공용 키를 이용하여 키를 암호화한다. 상기 키는 이것을 암호화할 수 있는 유일한 엔티티가 클리어링하우스(들)(105)이기 때문에, 콘텐츠(113)의 보안 없이도 어느 곳이나 전송될 수 있다.

126 이후, 암호화된 대칭 키, 메타데이터 및 콘텐츠(113)에 관한 다른 정보는 SC 패커 툴(152)에 의해 메타데이터 SC로 팩된다.

127 이후, 암호화된 콘텐츠(113) 및 메타데이터는 콘텐츠 SC로 팩된다. 이때, 콘텐츠(113)와 메타데이터에서의 처리가 완료된다.

128 이후, 메타데이터 SC(들)는 콘텐츠 배포 툴(도시되지 않음)을 이용하여 콘텐츠 프로모션 웹 사이트(156)에 전송된다.

129 콘텐츠 배포 툴은 콘텐츠 SC(들)를 콘텐츠 호스팅 사이트(들)(111)에 전송한다. 콘텐츠 호스팅 사이트(들)는 콘텐츠 제공자(들)(101), 클리어링하우스(들)(105) 또는 콘텐츠 호스팅을 위해 지정된 특정한 장소에 있을 수 있다. 상기 사이트에 대한 URL(Uniform Resource Locator)은 메타데이터 SC에 추가되어 있는 메타 데이터 부문이다.

130 콘텐츠 프로모션 웹 사이트(156)는 시스템(100)에 부가된 새로운 콘텐츠(113)를 전자 디지털 콘텐츠 스토어(들)(103)에 통지한다.

131 이후, 콘텐츠 취득 툴을 이용하여, 전자 디지털 콘텐츠 스토어(들)(103)는 판매하고자 하는 콘텐츠(113)에 해당하는 메타데이터 SC들을 다운로드시킨다.

132 전자 디지털 콘텐츠 스토어(들)(103)는 이들의 웹 사이트상에서 콘텐츠(들)(113)를 프로모션하기 위해 이용하고자 하는 메타데이터 SC(들)로부터 소정의 데이터를 추출하기 위해 콘텐츠 취득 툴을 이용할 수 있다. 상기 메타데이터 부문으로의 액세스는 원하는 경우에는 보안되어 과금될 수 있다.

133 상기 전자 디지털 콘텐츠 스토어(들)(103)의 특정한 콘텐츠(113)에 대한 사용 조건은 콘텐츠 취득 툴을 이용하여 기입된다. 상기 사용 조건은 소매 가격 및 콘텐츠(113)의 다른 압축 레벨에 대한 카피/플레이 제한을 포함한다.

134 전자 디지털 콘텐츠 스토어(들)(103)의 특정한 사용 조건 및 원 메타데이터 SC(들)는 SC 패커 툴에 의해 오퍼(offer) SC에 팩된다.

135 전자 디지털 콘텐츠 스토어(들)(103)의 웹 사이트가 갱신된 후, 콘텐츠(113)는 웹을 서핑하는 최종 사용자(들)에게 이용될 수 있다.

136 최종 사용자(들)가 자신이 구입하고자 하는 콘텐츠(113)를 발견했을 때, 이들은 음악 아이콘 같은 콘텐츠 아이콘을 클릭하고, 이 아이템은 전자 디지털 콘텐츠 스토어(들)(103)에 의해 유지되는 자신의 쇼핑 카트에 추가된다. 최종 사용자(들)가 쇼핑을 완료하면, 이들은 처리를 위해 전자 디지털 콘텐츠 스토어(들)(103)에 구매 요청을 제공한다.

137 이후, 전자 디지털 콘텐츠 스토어(들)(103)는 이들이 현재 사업하는 것과 동일한 방식으로 자금의 보유를 평가하기 위해 신용 카드 클리어링 조직과 상호작용한다.

138 일단, 전자 디지털 콘텐츠 스토어(들)(103)가 신용 카드 클리어링 조직으로부터 되돌아온 신용 카드 인증 번호를 수신하면, 이것

을 데이터베이스에 저장하고, 트랜잭션 SC를 구축하기 위해 SC 패커 툴을 불러온다. 상기 트랜잭션 SC는 최종 사용자(들)가 구입한 콘텐츠(113)에 대한 오퍼 SC들과, 전자 디지털 콘텐츠 스토어(들)(103)로 역추적될 수 있는 트랜잭션 ID와, 최종 사용자(들)를 식별하는 정보와, 압축 레벨과, 사용 조건 및 구입한 곡에 대한 가격표 모두를 포함한다.

139 이후, 상기 트랜잭션 SC가 최종 사용자 장치(들)(109)에 전송된다.

140 트랜잭션 SC가 최종 사용자 장치(들)(109)에 도달하면, 트랜잭션 SC를 여는 최종 사용자 플레이어 애플리케이션(195)을 작동시켜 최종 사용자의 구매를 승인한다. 이때, 최종 사용자 플레이어 애플리케이션(195)은 각 오퍼 SC들을 열며, 다른 실시예에서는 사용자에게 다운로드 시간의 추정치를 알려준다. 이후, 사용자는 자신이 콘텐츠(113)를 다운로드하고자 하는 때를 지정하기 위한 질문을 한다.

141 최종 사용자(들)가 다운로드를 요구하는 시간에 기초하여, 최종 사용자 플레이어 애플리케이션(195)은 특히 콘텐츠(113)에 대하여 암호화된 대칭 키, 트랜잭션 ID 및 최종 사용자(들) 정보를 포함한 오더 SC를 구축함으로써 다운로드 처리의 시작을 불러와서 개시할 수 있다.

142 이후, 상기 오더 SC는 처리를 위해 클리어링하우스(들)에 전송된다.

143 클리어링하우스(들)(105)는 오더 SC를 수신하고, 이것을 열어서, 어떠한 데이터도 변형되지 않았음을 검증한다. 클리어링하우스(들)(105)는 최종 사용자(들)에 의해 구입된 사용 조건을 확인한다. 상기 사용 조건은 콘텐츠 제공자(들)(101)에 의해 지정된 것에 따라야 한다. 상기 정보는 데이터베이스에 로그된다.

144 일단, 모든 검색이 완료되면, 암호화된 대칭 키는 클리어링하우스(들)(105)의 개인 키를 이용하여 해독된다. 이후, 대칭 키는 최종 사용자(들)의 공용 키를 이용하여 암호화된다. 이후, 상기 새로운 암호화된 대칭 키는 SC 패커에 의해 인가 SC에 패키징된다.

145 이후, 인가 SC는 최종 사용자(들)에 전송된다.

146 인가 SC가 최종 사용자 장치(들)(109)에서 수신되면, 이것은 콘텐츠 SC가 다운로드될 때까지 메모리에 저장된다.

147 최종 사용자 장치(들)(109)는 구입 콘텐츠(113)에 대한 대응하는 인가 SC를 전송하는 콘텐츠 호스팅 설비(111)로부터 요구한다.

148 콘텐츠(113)는 최종 사용자 장치(들)(109)에 전송된다. 수신시, 콘텐츠(113)는 대칭 키를 사용하여 최종 사용자 장치(들)에 의해 해독된다.

IV. 권리 관리 구조 모델

A. 구조 총 기능

도 5는 보안 디지털 콘텐츠 전자 배포 시스템(100)의 권리 관리 구조의 블록도이다. 구조적으로, 인가 제어층(501), 콘텐츠 식별층(503), 콘텐츠 사용 제어층(505) 및 콘텐츠 포매팅층(507)의 4개 층들이 보안 디지털 콘텐츠 전자 배포 시스템(100)을 나타낸다. 각 층의 전체적 기능적인 목적 및 각 층의 개별적 키 기능은 본 섹션에서 설명된다. 층들 각각의 기능은 다른 층들의 기능과 거의 독립적이다. 광범위한 제한 범위 내에서, 층의 기능은 다른 층의 기능에 영향을 주지 않으면서 유사한 기능으로 대체될 수 있다. 명확하게, 한 층으로부터의 출력은 인접 층에 허용가능한 포맷 및 시맨틱스를 충족해야만 한다.

인가 제어층(501)은 다음을 준수한다: 디지털 콘텐츠가 배포중에 불법적인 인터셉션 및 변형으로부터 보호된다.

- 콘텐츠(113)는 정당한 콘텐츠 소유자로부터 시작하여, 인가된 배포자인, 예컨대 전자 디지털 콘텐츠 스토어(들)(103)에 의해 배포된다.
- 디지털 콘텐츠 구매자는 정당하게 인가된 애플리케이션을 갖는다.
- 배포자는 콘텐츠(113)의 카피가 구매자 또는 최종 사용자(들)에게 이용될 수 있도록 하기 전에, 구매자에게서 비용을 지불받는다.
- 트랜잭션의 기록은 보고 목적으로 유지된다.

콘텐츠 식별층(503)은 콘텐츠 구매자의 동일성과 저작권의 검증을 허용한다. 콘텐츠의 저작권 정보 및 콘텐츠 구매자의 동일성은 소스가 인증되거나 인증되지 않은 소정의 콘텐츠(113)의 카피를 추적할 수 있도록 한다. 따라서, 콘텐츠 식별층(503)은 해적 행위에 대항하는 수단을 제공한다.

콘텐츠 사용 제어층(505)은 콘텐츠(113)의 카피가 스토어 사용 조건(519)에 따라 구매자의 장치에 이용되도록 한다. 스토어 사용 조건(519)은 콘텐츠(113)에 허용된 로컬 카피와, 플레이의 수 및, 콘텐츠(113)가 외부 휴대용 장치에 기록될 수 있는 가의 여부를 조건으로 지정할 수 있다. 콘텐츠 사용 제어층(505)의 기능은 콘텐츠의 카피/플레이 사용을 지속적으로 추적하고 카피/플레이 상태를 갱신하는 것이다.

콘텐츠 포매팅층(507)은 콘텐츠 소유자의 설비에서의 본래의 표현에서 보안 디지털 콘텐츠 전자 배포 시스템(100)의 배포 수단 및 서비스 특성과 일치하는 형태로 콘텐츠(113)의 포맷 변환을 허용한다. 변환 처리는 인코딩 및 이와 연관된 주파수 등화와 진폭의 동적인 조정 같은 전처리를 포함할 수 있다. 오디오인 콘텐츠(113)에 대하여, 구매자측에서 수신된 콘텐츠(113)는 또한 플레이백에 적합한 포맷을 얻거나 또는 휴대용 장치에 전송하기 위하여 처리될 필요가 있다.

B. 기능 분리 및 흐름

권리 관리 구조 모델은 도 5에 도시되며, 이것은 보안 디지털 콘텐츠 배포 시스템(100)을 구성하는 운영 성분에 대한 구조층의 맵핑 및 각 층에서의 키 기능을 예시한다.

1. 콘텐츠 포매팅층(507)

콘텐츠 포매팅층(507)에 연관된 포괄적인 기능으로는 콘텐츠 제공자(들)(101)에서의 전처리(502) 및 압축(511)과, 최종 사용자 장치(들)(109)에서의 스크램블링(513) 및 압축 해제(515)가 있다. 특정한 기능의 예와 전처리를 위한 요구는 상술하였다. 콘텐츠 압축(511)은 콘텐츠(113)의 파일 크기 및 그 전송 시간을 줄이기 위해 이용된다. 전송 매체와 콘텐츠(113)의 타입에 적합한 소정의 압축 알고리즘이 보안 디지털 콘텐츠 전자 배포 시스템(100)에 이용될 수 있다. 음악에서는, MPEG 1/4, 돌비 AC-2 및 AC-3, 소니 적응형 변환 코딩(ATRAC) 및 저-비트율 알고리즘이 통상적으로 이용되는 압축 알고리즘의 일부이다. 콘텐츠(113)는 저장 크기 요구 조건을 감소시키기 위해 압축된 형태로 최종 사용자 장치(들)(109)에 저장되며, 액티브 플레이백중에 압축 해제된다. 디스크램블링은 또한 액티브 플레이백중에 수행된다. 스크램블링의 타입 및 목적은 콘텐츠 사용 제어층(505)의 설명중에 후술된다.

2. 콘텐츠 사용 제어층(505)

콘텐츠 사용 제어층(505)은 콘텐츠(113)의 이용시 부여되는 제한 및 조건의 시행 및 명세가 최종 사용자 장치(들)(109)에서 이용되도록 허가한다. 조건은 콘텐츠(113)에 이용되는 플레이어의 횟수, 콘텐츠(113)의 이차 카피가 허용되는 가의 여부, 이차 카피의 횟수, 및 콘텐츠(113)가 외부 휴대 장치에 카피될 수 있는 가의 여부를 지정할 수 있다. 콘텐츠 제공자(들)(101)는 허용가능한 사용 조건(517)을 설정하고, 이들을 SC 내의 전자 디지털 콘텐츠 스토어(들)에 전송한다(인가 제어층(501) 섹션을 참조함). 전자 디지털 콘텐츠 스토어(들)(103)은 콘텐츠 제공자(들)(101)에 의해 설정된 원 조건에 비실효되지 않는 한 사용 조건(517)을 추가하거나 또는 줄일 수 있다. 이때, 전자 디지털 콘텐츠 스토어(들)(103)은 (SC 내의) 모든 스토어 사용 조건(519)을 최종 사용자 장치(들)(109) 및 클리어링하우스(들)(105)에 전송한다. 클리어링하우스(들)(105)는 최종 사용자 장치(들)(109)로의 콘텐츠(113) 릴리즈를 인증하기 전에 사용자 조건 검증(521)을 수행한다.

콘텐츠 사용 조건(517)의 집행은 최종 사용자 장치(들)(109)에 의해 수행된다. 우선, 최종 사용자 장치(들)(109)의 콘텐츠 식별층(503)으로부터 콘텐츠(113) 카피를 수신하면, 초기 카피/플레이 허가를 나타내는 카피/플레이 코드(523)로 콘텐츠(113)를 마크한다. 두 번째로, 플레이어 애플리케이션(195)은 최종 사용자 장치(들)(109)에 콘텐츠를 저장하기 전에 이 콘텐츠(113)를 암호적으로 스크램블한다. 플레이어 애플리케이션(195)은 각 콘텐츠 아이템마다 스크램블링 키를 생성하고, 키는 최종 사용자 장치(들)(109)에 암호화되어 숨겨진다. 이때, 최종 사용자 장치(들)(109)가 카피 또는 플레이를 위해 콘텐츠(113)에 액세스할 때마다, 최종 사용자 장치(들)(109)는 콘텐츠(113)의 디스크램블링 및 플레이 또는 카피의 실행을 허용하기 전에 카피/플레이 코드를 검증한다. 최종 사용자 장치(들)(109)는 또한 콘텐츠(113)의 최초의 카피에서 및 소정의 새로운 이차 카피상에서의 카피/플레이 코드를 적절하게 갱신한다. 카피/플레이 코딩은 압축된 콘텐츠(113)상에 수행된다. 즉, 카피/플레이 코드의 매입 전에 콘텐츠(113)를 압축 해제할 필요가 없다.

최종 사용자 장치(들)(109)는 콘텐츠(113) 내에 코드/플레이 코드를 매입하기 위해 인가 워터마크(527)를 이용한다. 매입 알고리즘 및 이와 연관된 스크램블링 키를 인식할 수 있는 최종 사용자 플레이어 애플리케이션(195)은 매입된 데이터를 판독 또는 변경할 수 있다. 데이터는 휴먼 관찰자에게 보이지 않거나 들리지 않는데, 즉 데이터는 콘텐츠(113)에 어떠한 감지할 수 있는 열화를 일으키지 않는다. 워터마크는 정상 콘텐츠 조작에 의해 일어나는 신호 열화, 콘텐츠 처리, 데이터 압축, D-to-A 및 A-to-D 변환의 여러 단계들에 잔류하기 때문에, 워터마크는 아날로그 표현을 포함한 소정의 표현 형태로 콘텐츠(113)에 남아있게 된다. 다른 실시예에서, 콘텐츠(113) 내에 카피/플레이 코드를 매입하기 위해 인가 워터마크(527)를 이용하는 대신에, 최종 사용자 플레이어 애플리케이션(195)은 안전하게 저장된 사용 조건(519)을 이용한다.

3. 콘텐츠 식별층(503)

콘텐츠 식별층(503) 부분에서, 콘텐츠 제공자(들)(101)는 또한 콘텐츠 식별자, 콘텐츠 소유자 및 발행일, 지리적 배포 지역 같은 다른 정보에 관하여 콘텐츠(113)에 데이터를 매입하기 위하여 인가 워터마크(527)를 이용한다. 이 워터마크는 여기서 저작권 워터마크(529)로 불린다. 수신시, 최종 사용자 장치(들)(109)는 콘텐츠 구매자의 이름, 트랜잭션 ID(535)(이하의 인가 제어층(501) 섹션을 참조함) 및 인가 일자 및 사용 조건(517) 같은 이외의 정보로 콘텐츠(113)의 카피를 워터마크한다. 상기 워터마크는 여기서는 인가 워터마크로 불린다. 인증된 방식이거나 아닌 방식으로 얻어지며 콘텐츠 품질을 유지하는 오디오 처리를 받는 콘텐츠(113)의 소정의 카피시에는 저작권 및 인가 워터마크가 수반된다. 콘텐츠 식별층(503)은 해적 행위를 방지한다.

4. 인가 제어층(501)

인가 제어층(501)은 콘텐츠(113)를 비인증된 인터셉션으로부터 방지하여, 콘텐츠가 최종 사용자 장치(들)(109)를 적절하게 인가하고 인증된 전자 디지털 콘텐츠 스토어(들)(103)와의 인가 구매 트랜잭션을 성공적으로 완성한 최종 사용자(들)에 각각 기초하여 릴리즈되도록 한다. 인가 제어층(501)은 이중 암호화(531)에 의해 콘텐츠(113)를 보호한다. 콘텐츠(113)는 콘텐츠 제공자(들)(101)에 의해 생성된 암호화 대칭 키를 이용하여 암호화되며, 대칭 키는 클리어링하우스(들)의 공용 키(621)를 이용하여 암호화된다. 클리어링하우스(들)(105)만이 초기에 대칭 키를 회복할 수 있다.

인가 제어부는 "신입된 대상"으로 클리어링하우스(들)(105)와 함께 디자인된다. 인가 요구(537)(즉, 최종 사용자 장치(들)(109))로의 콘텐츠(113)에 대한 대칭 키(623)에 대한 허가를 릴리즈하기 전에, 클리어링하우스(들)(105)는 트랜잭션 및 인가 인증(543)이 완전하고 진정한 것이며, 전자 디지털 콘텐츠 스토어(들)(103)가 전자 콘텐츠(113)의 판매를 위해 보안 디지털 콘텐츠 전자 배포 시스템(100)으로부터의 인증을 갖추며, 최종 사용자(들)가 정당하게 인가된 애플리케이션임을 검증한다. 감사/보고부(545)는 보고의 생성 및 보안 전자 디지털 콘텐츠 배포 시스템(100)에서 다른 인증된 대상들과 인가 트랜잭션 정보를 공유하도록 허용한다.

인가 제어는 SC 처리(533)를 통해 실행된다. SC(들)는 시스템 조작 성분들 사이의 정보 및 암호화된 콘텐츠(113)를 배포하기 위해 이용된다(SC(들)에 대해서는 이하에 구조 섹션에서 상세히 설명됨). SC는 비인증된 인터셉션 및 전자 정보 또는 콘텐츠(113)의 변형으로부터 보호하기 위하여 암호화, 디지털 기호 및 디지털 증명을 이용하는 정보의 암호화 캐리어이다. 또한, 전자 데이터의 정당성 검증을 허용한다.

인가 제어로 콘텐츠 제공자(들)(101), 전자 디지털 콘텐츠 스토어(들)(103) 및 클리어링하우스(들)(105)가 상기 성분을 인증하기 위해 이용되는 신뢰있는 증명 기관으로부터 진정한 암호화 디지털 증명서를 받을 수 있게 된다. 최종 사용자 장치(들)(109)는 디지털 증명서를 반드시 갖을 필요가 없다.

C. 콘텐츠 배포 및 인가 제어

도 6은 콘텐츠 배포 및 인가 제어의 개요 및 이것이 도 5의 인가 제어층에 적용됨을 예시한 블록도이다. 도면은 전자 디지털 콘텐츠 스토어(들)(103), 최종 사용자 장치(들)(109) 및 클리어링하우스(들)(105)가 인터넷을 통해 상호접속되고, 유니캐스트(포인트 투 포인트) 전송이 상기 성분들 사이에서 이용되는 경우를 도시한다. 콘텐츠 제공자(들)(101)와 전자 디지털 콘텐츠 스토어(들)(103) 간의 통신은 또한 인터넷과 또는 네트워크 상에서 이루어질 수 있다. 최종 사용자 장치(들)(109)와 전자 디지털 콘텐츠 스토어(들)(103) 간의 콘텐츠 구매 상거래 트랜잭션은 표준 인터넷 웹 프로토콜에 기초하는 것으로 가정한다. 웹 기반의 상호작용 부분으로서, 최종 사용자(들)는 구매를 위해 콘텐츠(113)의 선택을 하고, 개인 및 금융 정보를 제공하며, 구매 조건에 동의한다. 전자 디지털 콘텐츠 스토어(들)(103)는 SET 같은 프로토콜을 이용하여 취득 기관으로부터 지불 인증을 받을 수 있다.

도 6에서는 또한 전자 디지털 콘텐츠 스토어(들)(103)가 표준 웹 프로토콜 기반으로 최종 사용자 플레이어 애플리케이션(195)에서, 최종 사용자 장치(들)(109)로 다운로드시키는 것으로 가정한다. 구조는 전자 디지털 콘텐츠 스토어(들)(103)가 유일 애플리케이션 ID를 다운로드된 플레이어 애플리케이션(195)에 할당하고, 최종 사용자 장치(들)(109)가 이것을 다음의 애플리케이션 인가 검증(하기)에 참조)을 위해 저장하도록 해야한다.

전체 인가 흐름은 콘텐츠 제공자(들)(101)에서 시작된다. 콘텐츠 제공자(들)(101)는 국부적으로 생성된 암호화 대칭 키를 이용하여 콘텐츠(113)를 암호화하고, 클리어링하우스(들)(105)의 공용 키(621)를 이용하여 대칭 키(623)를 암호화한다. 다른 실시예에서는, 대칭 키가 국부적으로 생성되는 대신에 클리어링하우스(들)(105)로부터 콘텐츠 제공자(들)(101)로 전송된다. 콘텐츠 제공자(들)(101)는 암호화된 콘텐츠(113) 주위에 콘텐츠 SC(들)(630), 및 암호화된 대칭 키(623), 스토어 사용 조건(519) 및 연관된 정보를 갖는 다른 콘텐츠(113) 주위에 메타 데이터 SC(들)(620)를 생성한다. 모든 콘텐츠(113) 객체마다 하나의 메타 데이터 SC(들)(620) 및 하나의 콘텐츠 SC(들)(630)가 있다. 콘텐츠(113) 객체는 압축 레벨이 동일한 하나의 곡이거나, 또는 콘텐츠(113)는 앨범에서의 각 곡일 수 있거나, 또는 콘텐츠(113)는 전체 앨범일 수 있다. 각 콘텐츠(113) 객체에 대하여, 메타 데이터 SC(들)(620)는 또한 콘텐츠 사용 제어층(505)과 연관된 스토어 사용 조건(519)을 수반한다.

콘텐츠 제공자(들)(101)는 메타 데이터 SC(들)(620)를 하나 이상의 전자 디지털 콘텐츠 스토어(들)(103)에 배포하고(스텝 601), 콘텐츠 SC(들)(630)를 하나 이상의 콘텐츠 호스팅 사이트에 배포한다(스텝 602). 다음에, 각 전자 디지털 콘텐츠 스토어(들)(103)는 오퍼 SC(들)(641)를 생성한다. 오퍼 SC(들)(641)는 일반적으로 콘텐츠 제공자(들)(101)의 디지털 기호(624) 및 (콘텐츠 제공자(들)(101)의 도시되지 않은)증명서를 포함한 메타 데이터 SC(들)(620)와 같이 많은 정보를 수반한다. 상술된 바와 같이, 전자 디지털 콘텐츠 스토어(들)(103)는 초기에 콘텐츠 제공자(들)(101)에 의해 규정된 (제어 사용 제어층에 의해 조정되는)스토어 사용 조건(519)을 추가하거나 또는 좁힐 수 있다. 선택적으로, 콘텐츠 SC(들) 및/또는 메타 데이터 SC(들)(620)는 콘텐츠 제공자(들)(101)의 디지털 기호(624)로 부호화된다.

최종 사용자 장치(들)(109)와 전자 디지털 콘텐츠 스토어(들)(103) 상의 콘텐츠 구매 트랜잭션을 완료한 후(스텝 603), 전자 디지털 콘텐츠 스토어(들)(103)는 트랜잭션 SC(들)(640)를 생성하여 최종 사용자 장치(들)(109)에 전송한다(스텝 604). 트랜잭션 SC(들)(640)는 유일 트랜잭션 ID(535), 구매자의 이름(즉, 최종 사용자(들)의 이름)(도시되지 않음), 최종 사용자 장치(들)(109)의 공용 키(661) 및 구매 콘텐츠(113)와 연관된 오퍼 SC(들)(641)를 포함한다. 도 6에서의 트랜잭션 데이터(642)는 트랜잭션 ID(535) 및 최종 사용자(들) 이름(도시되지 않음)을 모두 나타낸다. 트랜잭션 데이터(642)는 클리어링하우스(들)(105)의 공용 키(621)로 암호화된다. 선택적으로, 트랜잭션 SC(들)(640)는 전자 디지털 콘텐츠 스토어(들)(103)의 디지털 기호(643)로 부호화된다.

트랜잭션 SC(들)(및 이것에 포함된 오퍼 SC(들)(641))의 수신시, 최종 사용자 장치(들)(109)상에서 실행되는 최종 사용자 플레이어 애플리케이션(195)은 오더 SC(들)(650)에 의해 클리어링하우스(들)로부터의 인가 인증을 요구한다(스텝 605). 오더 SC(들)(650)는 오더 SC(들)(641)로부터의 암호화된 대칭 키(623) 및 스토어 사용 조건(519)과, 트랜잭션 SC(들)(640)로부터의 암호화된 트랜잭션 데이터(642), 및 최종 사용자 장치(들)(109)로부터의 암호화된 애플리케이션 ID(551)를 포함한다. 다른 실시예에서, 오더 SC(들)(650)는 최종 사용자 장치(들)(109)의 디지털 기호(652)로 부호화된다.

최종 사용자 장치(들)(109)로부터 오더 SC(들)(650)를 수신하면, 클리어링하우스(들)(105)는 다음을 검증한다: 1. 전자 디지털 콘텐츠 스토어(들)(103)가 보안 디지털 콘텐츠 전자 배포 시스템(100)으로부터의 인증(클리어링하우스(들)(105)의 데이터베이스(160)에 존재함)을 갖음;

2. 오더 SC(들)가 변경되지 않았음;

3. 트랜잭션 데이터(642) 및 대칭 키(623)가 완전하고 정당한 것임;

4. 최종 사용자 장치(들)(109)에 의해 구매된 전자 스토어 사용 조건(519)이 콘텐츠 제공자(들)(101)에 의해 설정된 상기 사용 조건(517)과 일치함; 및

5. 애플리케이션 ID(551)가 유효한 구성을 갖으며, 인증된 전자 디지털 콘텐츠 스토어(들)(103)에 의해 제공됨.

만약, 검증이 성공적이라면, 클리어링하우스(들)(105)는 대칭 키(623)를 해독하고, 트랜잭션 데이터(642)는 인가 SC(들)(660)를 구축하여 최종 사용자 장치(들)(109)에 전송한다(스텝 606). 인가 SC(들)(660)는 최종 사용자 장치(들)(109)의 공용 키(661)를 이용하여 모두 암호화되는 대칭 키(623) 및 트랜잭션 데이터(642)를 수반한다. 만약, 소정의 검증이 성공적이지 않다면, 클리어링하우스(들)(105)는 최종 사용자 장치(들)(109)에 인가를 거부하고, 이를 최종 사용자 장치(들)(109)에 통보한다. 클리어링하우스(들)(105)는 또한 상기 검증 실패를 전자 디지털 콘텐츠 스토어(들)(103)에 바로 통보한다. 다른 실시예에서, 클리어링하우스(들)(105)는 그 디지털 기호(663)로 인가 SC(들)(660)을 부호화한다.

인가 SC(들)(660)를 수신한 후, 최종 사용자 장치(들)(109)는 클리어링하우스(들)(105)로부터 미리 수신된 대칭 키(623) 및 트랜잭션 데이터(642)를 해독하고, 콘텐츠 호스팅 사이트(들)(111)로부터 콘텐츠 SC(들)를 요구한다(스텝 607). 콘텐츠 SC(들)(630)의 도달시(스텝 608), 최종 사용자 장치(들)(109)는 대칭 키(623)를 이용하여 콘텐츠(113)를 해독하고(스텝 609), 도 5에 대하여 이미 설명된 바와 같이 인가 워터마킹, 카피/플레이 코딩, 스크램블링 및 다른 콘텐츠(113) 처리를 위해 콘텐츠(113) 및 트랜잭션 데이터(642)를 다른 층에 전달한다.

마지막으로, 클리어링하우스(들)(105)는 감사 및 추적 목적을 위해 콘텐츠 제공자(들)(101) 및 전자 디지털 콘텐츠 스토어(들)(103)에 요약 트랜잭션 보고를 주기에 기초하여 전송한다(스텝 610).

V. 보안 컨테이너 구성

A. 일반 구성

보안 컨테이너(SC)는 콘텐츠(113)의 단위 또는 일부 트랜잭션을 함께 규정하고, 또한 사용 조건, 메타 데이터 및 암호화 방법 같은 관련 정보를 규정하는 여러 가지 부분들로 이루어진 구성이다. SC(들)는 정보의 무결성, 완전성 및 정당성이 검증될 수 있도록 하는 방식으로 디자인된다. SC(들) 내의 정보중 일부는 정당한 인증이 확보된 후에만 액세스될 수 있도록 암호화될 수 있다.

SC(들)는 SC(들) 및 SC(들) 내에 포함된 부분들 각각에 관한 정보의 기록을 갖는 적어도 하나의 자료의 빌(BOM) 부분을 포함한다. 메시지 다이제스트는 각 부문에 대하여 MD-5 같은 해시 알고리즘을 이용하여 계산된 다음, 그 부문에 대한 BOM 기록에 포함된다. 부문의 다이제스트는 함께 연결되며, 다른 다이제스트는 이들로부터 계산된 다음, 디지털 기호를 생성하기 위하여 SC(들)를 생성하는 엔티티의 개인 키를 이용하여 암호화된다. SC(들)를 수신한 대상은 모든 다이제스트를 검증하기 위하여 디지털 기호를 이용할 수 있으며, 따라서 SC(들) 및 그 부분들 모두의 무결성 및 완전성을 확인한다.

다음의 정보는 각 부문에 대한 기록과 함께 BOM에서의 기록으로 포함될 수 있다. SC(들) 타입은 기록에 다음의 것들이 포함될 필요가 있음을 결정한다:

- SC(들) 버전 • SC(들) ID • SC(들)의 타입(예컨대, 오퍼, 오더, 트랜잭션, 콘텐츠, 메타 데이터 또는 프로모션 및 인가) • SC(들)의 발행자 • SC(들)이 생성된 데이터 • SC(들)의 만료일 • 클리어링하우스(들) URL • 포함된 부문에 이용되는 다이제스트 알고리즘의 설명(디폴트는 MD-5임) • 디지털 기호 암호화를 위해 이용되는 알고리즘의 설명(디폴트는 RSA임) • 디지털 기호(포함된 부분들의 모든 연결된 다이제스트들중 암호화된 다이제스트)SC(들)는 하나 이상의 BOM을 포함할 수 있다. 예를 들면, 오퍼 SC(들)(641)는 전자 디지털 콘텐츠 스토어(들)(103)에 의해 부가된 정보와 함께 그 BOM 및 새로운 BOM을 포함한 원 메타 데이터 SC(들)(620) 부분들로 구성된다. 상기 기록은 그 무결성을 확인하기 위해 이용될 수 있는 메타 데이터 SC(들)(620) BOM에 대한 다이제스트를 포함하고, 따라서 메타 데이터 SC(들)(620)로부터 포함된 부분들의 무결성이 또한 메타 데이터 SC(들)(620) BOM에 저장된 부문 다이제스트 값을 이용하여 확인될 수 있다. 메타 데이터 SC(들)(620)로부터의 어떠한 부분들도 오퍼 SC(들)(641)에 생성되었던 새로운 BOM에 기록을 갖지 않는다. 전자 디지털 콘텐츠 스토어(들)(103) 및 메타 데이터 SC(들)(620) BOM에 의해 부가된 부분들만이 새로운 BOM에 기록을 갖는다.

SC(들)는 또한 키 설명 부문을 포함한다. 키 설명 부문은 SC(들) 내의 암호화된 부문들에 관한 다음의 정보를 갖는 기록을 포함한다.

- 암호화된 부문의 이름.
- 해독화될 때 상기 부문을 이용하기 위한 이름.
- 상기 부문을 암호화하기 위해 이용된 암호화 알고리즘.
- 상기 부문을 암호화하기 위해 이용된 공용 암호화 키를 나타내기 위한 키 식별자, 또는 해독될 때 암호화된 부문을 해독하기 위해

이용되는 암호화된 대칭 키.

- 대칭 키를 암호화하기 위해 이용된 암호화 알고리즘. 이 필드는 키 설명 부문에서의 기록이 암호화된 부문을 암호화하기 위하여 이용된 암호화된 대칭 키를 포함할 때만 존재한다.

- 대칭 키를 암호화하기 위해 이용된 공용 암호화 키의 키 식별자. 이 필드는 키 설명 부문에서의 기록이 암호화된 대칭 키 및 암호화된 부문을 암호화하기 위하여 이용된 대칭 키의 암호화 알고리즘 식별자를 포함할 때만 존재한다.

SC(들)가 소정의 암호화된 부문들을 포함하지 않으면, 이때는 키 설명 부문이 없다.

B. 권리 관리 언어 신택스 및 시멘틱스

권리 관리 언어는 콘텐츠(113) 구매 후 최종 사용자(들)에 의해 콘텐츠(113) 이용 제한을 규정하기 위한 값으로 할당될 수 있는 파라미터들로 구성된다. 콘텐츠(113) 이용 제한은 사용 조건(517)이다. 각 콘텐츠 제공자(들)(101)는 그 콘텐츠(113) 아이템들 각각에 대한 사용 조건(517)을 지정한다. 전자 디지털 콘텐츠 스토어(들)(103)는 메타 데이터 SC(들)(620)에서의 사용 조건(517)을 해석하고, 그 정보를 이용하여 콘텐츠(113)에 대한 소매 구매 정보를 부가함과 함께 그들이 그들의 고객을 오픈하고자 하는 선택을 제공하기 위해 정보를 이용한다. 최종 사용자(들)가 구매를 위한 콘텐츠(113) 아이템을 선택한 후, 최종 사용자 장치(들)(109)는 스토어 사용 조건(519)에 기초하여 콘텐츠에 대한 인증을 요구한다. 클리어링하우스(들)(105)가 최종 사용자(들)에게 인증 SC(들)(660)를 전송하기 전에, 클리어링하우스(들)(105)는 요구된 스토어 사용 조건(519)이 콘텐츠 제공자(들)(101)에 의해 메타 데이터 SC(들)(620)로 지정된 허용가능한 사용 조건(517)과 일치함을 검증한다.

최종 사용자 장치(들)(109)가 구매한 콘텐츠(113)를 수신하면, 스토어 사용 조건(519)은 워터마킹 툴을 이용하여 상기 콘텐츠(113)에 인코딩되거나, 또는 안전하게 저장된 사용 조건(519)으로 인코딩된다. 최종 사용자 장치(들)(109)상에서 실행되는 최종 사용자 플레이어 애플리케이션(195)은 콘텐츠(113)로 인코딩되었던 스토어 사용 조건(519)이 집행되도록 한다.

다음은 콘텐츠(113)가 음악인 경우에 실시예에서의 스토어 사용 조건(519)의 예이다: • 곡이 녹음가능함.

- 곡이 n번 플레이될 수 있음.

C. 보안 컨테이너 흐름 및 처리의 개요

메타 데이터 SC(들)(620)는 콘텐츠 제공자(들)(101)에 의해 구축되며, 곡 같은 콘텐츠(113) 아이템을 규정하기 위해 이용된다. 콘텐츠(113) 자체가 상기 SC(들)에 포함되지 않는데, 그 이유는 콘텐츠(113)의 크기가 일반적으로 전자 디지털 콘텐츠 스토어(들)(103) 및 최종 사용자(들)에게는 너무 커서 설명적인 메타 데이터의 액세스성 목적으로만 컨테이너를 효과적으로 다운로드할 수 없기 때문이다. 대신에, SC(들)는 콘텐츠(113)로의 지정을 위한 외부 URL(유니폼 리소스 로케이터)을 포함한다. SC(들)는 또한 콘텐츠(113)에 관한 설명적 정보, 및 예컨대 음악에서의 CD 표지 및/또는 곡 콘텐츠(113)의 경우에는 디지털 오디오 클립 같은 소정의 다른 연관된 데이터를 포함한다.

전자 디지털 콘텐츠 스토어(들)(103)는 인증된 메타 데이터 SC(들)(620)를 다운로드하고, 오퍼 SC(들)(641)를 구축한다. 요컨대, 오퍼 SC(들)(641)는 전자 디지털 콘텐츠 스토어(들)(103)에 의해 포함된 부가 정보와 함께 메타 데이터 SC(들)(620)로부터 BOM과 일부 부문들로 구성된다. 오퍼 SC(들)(641)에 대한 새로운 BOM은 오퍼 SC(들)(620)가 구축될 때 생성된다. 전자 디지털 콘텐츠 스토어(들)(103)는 또한 콘텐츠(113)의 설명이 최종 사용자(들)에게 나타나는 웹 사이트상에 HTML 페이지를 구축하기 위해 상기 스토어로부터 메타 데이터 정보를 추출함으로써 메타 데이터 SC(들)(620)를 이용하고, 일반적으로 이와 같이 하여 콘텐츠(113)를 구매할 수 있다.

전자 디지털 콘텐츠 스토어(들)에 의해 부가된 오퍼 SC(들) 내의 정보는 일반적으로 메타 데이터 SC(들)(620)와 스토어의 웹 사이트로의 URL 및 스토어 로고의 그래픽 영상 같은 프로모션형 데이터에 지정된 사용 조건(517)의 선택을 좁히기 위한 것이다. 메타 데이터 SC(들)(620) 내의 오퍼 SC(들)(641) 템플릿은, 정보가 오퍼 SC(들)(641)에서 전자 디지털 콘텐츠 스토어(들)(103)에 의해 무시될 수 있고, 만약 무시된다면, 어떠한 부가 정보가 전자 디지털 콘텐츠 스토어(들)(103)에 의해 요구되며, 어떠한 부문들이 매입된 메타 데이터 SC(들)(620)에 보유되는 지를 나타낸다.

오퍼 SC(들)(641)는 최종 사용자(들)가 전자 디지털 콘텐츠 스토어(들)(103)로부터 콘텐츠(113)를 구매하기로 결정할 때 트랜잭션 SC(들)(640)에 포함된다. 전자 디지털 콘텐츠 스토어(들)(103)는 트랜잭션 SC(들)(640)을 구축하고, 구매될 각 콘텐츠(113) 아이템에 대한 오퍼 SC(들)(641)를 포함하며, 이것을 최종 사용자 장치(들)(109)에 전송한다. 최종 사용자 장치(들)(109)는 트랜잭션 SC(들)(640)을 수신하고, 트랜잭션 SC(들)(640)와 이에 포함된 오퍼 SC(들)(641)의 무결성을 확인한다.

오더 SC(들)(650)는 구매되는 각 콘텐츠(113) 아이템마다 최종 사용자 장치(들)(109)에 의해 구축된다. 정보는 오퍼 SC(들)(641), 트랜잭션 SC(들)(640) 및 최종 사용자 장치(들)(109)의 구성 파일로부터 포함된다. 오더 SC(들)(650)는 동시에 클리어링하우스(들)(105)에 전송된다. 클리어링하우스(들)(105) URL에서 오더 SC(들)(650)는 메타 데이터 SC(들)(620)에 대한 BOM에서의 기록중 하나로서 포함되며 오퍼 SC(들)(641)에도 다시 포함된다.

클리어링하우스(들)(105)는 인가 워터마크(527)에 필요한 모든 것들을 최종 사용자 장치(들)(109)에 공급하기 위해 오더 SC(들)(650)를 확인하여 처리하며, 구매한 콘텐츠(113)에 액세스한다. 클리어링하우스(들)(105)의 기능중 하나는 콘텐츠 SC(들)(630)로부터의 콘텐츠(113), 및 오퍼 SC(들)(641)로부터의 워터마킹 명령을 해독하기 위해 필요한 대칭 키(623)를 해독하기 위한 것이다. 암

호화된 대칭 키(623) 기록은 실질적으로 실제의 암호화된 대칭 키(623) 보다 많은 것을 포함한다. 암호화를 실행하기 전에, 콘텐츠 제공자(들)(101)는 실제의 대칭 키(623)에 그 이름을 선택적으로 첨부할 수 있다. 대칭 키(623)와 함께 암호화된 콘텐츠 제공자(들)(101)의 이름을 갖으면, 합법적 SC(들)로부터 자체적으로 메타 데이터 SC(들)(620) 및 콘텐츠 SC(들)(630)를 구축한 콘텐츠 제공자(들)(101)로의 해적 행위에 대한 보안을 제공할 수 있다. 클리어링하우스(들)(105)는 대칭 키(623)와 함께 암호화된 콘텐츠 제공자(들)(101)의 이름이 SC(들) 증명서에서의 콘텐츠 제공자(들)(101)의 이름과 일치하는 가를 확인한다.

만약, 클리어링하우스(들)(105)에 의한 워터마킹 명령에 소정의 변화가 필요하다면, 이때 클리어링하우스(들)(105)는 대칭 키(623)를 해독하고, 워터마킹 명령을 수정하고, 새로운 대칭 키(623)를 이용하여 이들을 다시 암호화한다. 이후, 대칭 키(623)는 최종 사용자 장치(들)(109)의 공용 키(661)를 이용하여 재암호화된다. 클리어링하우스(들)(105)는 또한 SC(들) 내의 다른 대칭 키(623)를 해독하고, 최종 사용자 장치(들)(109)의 공용키(661)로 이들을 다시 암호화한다. 클리어링하우스(들)(105)는 새로이 암호화된 대칭 키(623) 및 갱신된 워터마킹 명령을 포함한 인가 SC(들)(660)를 구축하고, 이것을 오더 SC(들)(650)에 응답하여 최종 사용자 장치(들)(109)에 전송한다. 오더 SC(들)의 처리가 완전하게 완성되지 않으면, 이때 클리어링하우스(들)(105)는 최종 사용자 장치(들)(109)의 HTML 페이지로 되돌아가거나, 또는 인증 처리의 실패를 알린다.

인가 SC(들)(660)는 콘텐츠(113) 아이템에 액세스하기 위해 필요한 모든 것을 최종 사용자 장치(들)(109)에 제공한다. 최종 사용자 장치(들)(109)는 콘텐츠 호스팅 사이트(들)(111)로부터 적절한 콘텐츠 SC(들)(630)를 요구한다. 콘텐츠 SC(들)(630)는 콘텐츠 제공자(들)(101)에 의해 구축되며, 암호화된 콘텐츠(113) 및 메타 데이터 부분들을 포함한다. 최종 사용자 플레이어 애플리케이션(195)은 콘텐츠(113), 메타 데이터 및 워터마킹 명령을 해독하기 위해 인가 SC(들)(660)에서의 대칭 키(623)를 이용한다. 이때, 워터마킹 명령은 콘텐츠(113)에 첨부되고, 콘텐츠(113)는 최종 사용자 장치(들)(109)상에 스크램블되어 기억된다.

D. 메타 데이터 보안 컨테이너(620) 포맷

다음의 표는 메타 데이터 SC(들)(620)에 포함된 부분들을 도시한다. 이 부문 열에서의 각 박스는 BOM과 함께(□ 문자로 둘러싸인 부문명은 제외함) SC(들)에 포함된 독립적 객체이다. BOM은 SC(들)에 포함된 각 부문에 대한 기록을 갖는다. 부문 존재 열은 부문 자체가 실질적으로 SC(들)에 포함되는가의 여부를 나타내고, 다이제스트 열은 메시지 다이제스트가 부문마다 계산되는가의 여부를 나타낸다. 일부 부문들은, 전체 원 BOM이 전달되더라도 (연관된 템플릿에 의해 결정됨에 따라) SC(들)가 다른 SC(들)에 포함되면, 전달될 수 없다. 이것은 전체 BOM이 원 SC(들)에서의 디지털 기호를 검증하기 위해 클리어링하우스(들)(105)에 의해 요구되기 때문에 이루어진다.

다음의 표의 키 설명 부문 열은 SC(들)의 키 설명 부문에 포함된 기록을 정의한다. 키 설명 부문에서의 기록은 SC(들) 내의 부문들 또는 다른 SC(들) 내의 부문을 암호화하기 위해 이용된 알고리즘 및 암호화 키에 관한 정보를 정의한다. 각 기록은 암호화된 부문명을 포함하고, 필요하다면, 다른 SC(들)를 지시하는 URL이 암호화된 부문을 포함한다. 결과명 열은 해독된 후에 부문에 할당된 이름을 정의한다. 암호화 알고리즘 열은 부문을 암호화하기 위해 이용된 암호화 알고리즘을 정의한다. 키 Id/Enc 키 열은 부문을 암호화하기 위해 이용된 암호화 키의 식별 또는 부문을 암호화하기 위해 이용된 암호화된 대칭 키(623) 비트 스트링의 기본 64 인코딩을 정의한다. Sym Key Alg 열은, 이전의 열이 암호화된 대칭 키(623)일 때, 대칭 키(623)를 암호화하기 위해 이용된 암호화 알고리즘을 정의하는 선택적 파라미터이다. Sym Key ID 열은, Key Id/Enc Key 열이 암호화된 대칭 키(623)일 때, 대칭 키(623)를 암호화하기 위해 이용된 암호화 키의 식별이다.

부문

BCM

키 설명 부문

부문 존재

다이제스트

결과명

암호화 알고리즘

Key ID/Enc Key

Sym Key Alg

Sym Key ID

[콘텐츠 URL]
[메타데이터 URL]

출력 부문	RCA	Enc Sym Key	RSA	CH Pub Key
출력 부문	RCA	Enc Sym key	RSA	CH Pub Key

SC 버전	
SC ID	
SC 타입	
SC 발행자	
일자	
만료일	
클리어링하우스(들) URL	
다이제스트 알고리즘 ID	
디지털 기호 알고리즘 ID	
Yes	Yes
Yes	Yes
Yes	Yes
Yes	Yes
Yes	Yes
Yes	Yes
Yes	Yes
Yes	No
Yes	No

콘텐츠 ID
메타데이터
사용조건
SC 템플릿
위터마킹 명령
키 설명 부문
클리어링하우스(들) 증명서(들)
증명서(들)

출력 부문	RCA	Enc Sym key	RSA	CH Pub Key
-------	-----	-------------	-----	------------

디지털 기호

다음은 상기 메타 데이터 SC(들) 표에 이용된 용어를 설명한다: •[콘텐츠-URL] - 키 설명 부문의 기록에서의 파라미터. 이것은 상기 메타 데이터 SC(들)(620)와 연관된 콘텐츠 SC(들)(630)에서의 암호화된 콘텐츠(113)를 지시하는 URL이다. 메타 데이터 SC(들)(620) 자체는 암호화된 콘텐츠(113)를 포함하지 않는다.

• [메타 데이터 URL] - 키 설명 부문의 기록에서의 파라미터. 이것은 상기 메타 데이터 SC(들)(620)와 연관된 콘텐츠 SC(들)(630)에서의 암호화된 메타 데이터에 지시하는 URL이다. 메타 데이터 SC(들)(620)는 자체적으로 암호화된 메타 데이터를 포함하지 않는다.

• 콘텐츠 ID - 콘텐츠(113) 아이템에 할당된 유일 ID를 정의하는 부문. 메타 데이터 SC(들)(620)가 하나 이상의 콘텐츠(113) 아이템을 설명하는 경우, 상기 부문에 포함된 하나 이상의 콘텐츠 ID가 있다.

• 메타 데이터 - 곡의 경우에 가수명 및 CD 표지 그림 같은 콘텐츠(113) 아이템에 관한 정보를 포함하는 부문. 일부가 암호화될 수 있는 다중 메타 데이터 부문이 있을 수 있다. 메타 데이터 부문의 내부 구조는 그 안에 포함된 메타 데이터의 타입에 따라 다르다.

• 사용 조건 - 콘텐츠(113)의 이용을 위해 최종 사용자(들)에 부여될 수 있는 사용 옵션, 규칙 및 제한을 설명하는 정보를 포함하는 부문.

• SC(들) 템플릿 - 오퍼, 오더 및 인가 SC(들)(660)를 구축하기 위한 필수적인 정보와 선택적인 정보를 설명하는 템플릿을 정의하는 부문.

• 위터마킹 명령 - 콘텐츠(113)에 위터마킹을 실행하기 위해 암호화된 명령 및 파라미터를 포함한 부문. 위터마킹 명령은 클리어링 하우스(들)(105)에 의해 수정될 수 있으며, 인가 SC(들)(660) 내의 최종 사용자 장치(들)(109)로 되돌아갈 수 있다. 위터마킹 명령을 암호화하기 위해 이용된 암호화 알고리즘, 위터마킹 명령이 해독될 때 이용하기 위한 출력 부문 명칭, 위터마킹 명령을 암호화하기 위해 이용되는 암호화된 대칭 키(623) 비트 스트링의 기본 64 인코딩, 대칭 키(623)를 암호화하기 위해 이용되는 암호화 알고리즘, 및 대칭 키(623)를 해독하기 위해 필요한 공용 키 식별시의 기록이 있다.

• 클리어링하우스(들) 증명서(들) - 클리어링하우스(들)(105)의 부호화된 공용 키(621)를 포함한 클리어링하우스(들)(105)로부터 또는 증명 기관으로부터의 증명서. 이때, 하나 이상의 증명서가 있을 수 있는데, 이 경우, 계층적 레벨 구성은 클리어링하우스(들)(105)의 공용 키(621)를 포함하여 도달되는 다음의 최저 레벨 증명서를 공개하기 위해 공용 키를 갖는 최고 레벨 증명서로 이용된다.

• 증명서(들) - SC(들)를 생성한 엔티티의 부호화된 공용 키(621)를 포함한 클리어링하우스(들)(105)로부터 또는 증명 기관으로부터의 증명서. 이때, 하나 이상의 증명서가 있을 수 있는데, 이 경우, 계층적 레벨 구성은 SC(들) 생성기의 공용 키를 포함한 최저 레벨 증명서가 도달될 때까지 다음 레벨의 증명서 등을 공개하기 위한 공용 키를 갖는 최고 레벨 증명서로 이용된다.

• SC 버전 - SC 패커 틀에 의해 SC(들)에 할당된 버전 번호.

• SC ID - SC(들)를 생성한 엔티티에 의해 SC(들)에 할당된 유일 ID.

- SC 타입 - SC(들)의 타입(예컨대, 메타 데이터, 오퍼, 오더 등)을 표시함.
 - SC 발행자 - SC(들)를 생성한 엔티티를 표시함.
 - 생성일 - SC(들)가 생성된 일자.
 - 만료일 - SC(들)가 만료되어 더 이상 유효하지 않은 일자.
 - 클리어링하우스(들) URL - 최종 사용자 플레이어 애플리케이션(195)이 콘텐츠(113)에 액세스하기 위한 적절한 기관을 확보하기 위해 상호작용해야 하는 클리어링하우스(들)(105)의 어드레스.
 - 다이제스트 알고리즘 ID - 부분들의 다이제스트를 계산하기 위해 이용되는 알고리즘의 식별자.
 - 디지털 기호 Alg ID - 연결된 부문 다이제스트들의 다이제스트를 암호화하기 위해 이용되는 알고리즘의 식별자.
 - 디지털 기호 - SC(들)를 생성한 엔티티의 공용 키로 암호화된 연결된 부문 다이제스트들의 다이제스트.
 - 출력 부문 - 암호화된 부문이 해독될 때, 출력 부문에 할당된 이름.
 - RSA 및 RC4 - 대칭 키(623) 및 데이터 부문을 암호화하기 위해 이용되는 디폴트 암호화 알고리즘.
 - Enc Sym Key - 해독될 때, SC(들) 부문을 해독하기 위해 이용되는 암호화된 키 비트 스트림의 기본 64 인코딩.
 - CH Pub Key - 클리어링하우스(105)의 공용 키(621)가 데이터를 암호화하기 위해 이용됨을 표시한 식별자.
 - E. 오퍼 보안 컨테이너(641) 포맷
- 다음의 표는 오퍼 SC(들)(641)에 포함된 부문을 보여준다. 메타 데이터 SC(들)(620)로부터 BOM 및 일부 메타 데이터를 제외한 부문들은 또한 오퍼 SC(들)(641)에 포함된다.

부문

부문 존자

다이제스트

결과명

암호화 알고리즘

키 설명 부문

Key ID/Enc Key

Sym Key Alg

Sym Key ID

메타데이터 SC 부문

[콘텐츠 URL]

[메타데이터 URL]

출력 부문

RCA

Enc Sym Key

RSA

CH Pub Key

출력 부문

RCA

Enc Sym key

RSA

CH Pub Key

SC 버전

SC ID

SC 타입

SC 발행자

일자

만료일

클리어링하우스(들) URL

다이제스트 알고리즘 ID

디지털 기호 알고리즘 ID

Yes

Yes

Some

Yes

Yes

Yes

Yes

Yes

Yes

Yes

Yes

No

Yes

No

디지털 기호

출력 부문

RCA

Enc Sym key

RSA

CH Pub Key

오퍼 SC 부문

SC 버전

SC ID

SC 타입

SC 발행자

일자

만료일

다이제스트 알고리즘 ID

디지털 기호 알고리즘 ID

Yes

Yes

Yes

Yes

Yes

No

Yes

No

디지털 기호

메타데이터

부가 및 무시 필드

전자 디지털 콘텐츠

스토어(들) 증명서

증명서(들)

다음은 다른 SC(들)에 대하여 이전에 설명되지 않은 상기 오퍼 SC(들) (641)에서 이용되는 용어를 설명한다:

- 메타-데이터 SC(들) BOM - 원 메타 데이터 SC(들)(620)로부터의 BOM. 오퍼 SC(들)(641) BOM에서의 기록은 메타 데이터 SC(들)(620) BOM의 다이제스트를 포함한다.
- 부가 또는 무시 필드 - 전자 디지털 콘텐츠 스토어(들)(103)에 의해 무시된 사용 조건 정보. 이 정보는 전자 디지털 콘텐츠 스토어(들)(103)가 무시한 것이 그 인증 범위 내에 있음을 확인하기 위하여 수신된 SC(들) 템플릿을 통해 클리어링하우스(들)(105)에 의해 검증된다.
- 전자 디지털 콘텐츠 스토어(들) 증명서 - 클리어링하우스(들)(105)에 의해 전자 디지털 콘텐츠 스토어(들)(103)에 제공되고, 그 개인 키를 이용하여 클리어링하우스(들)(105)에 의해 부호화된 증명서. 이 증명서는 전자 디지털 콘텐츠 스토어(들)(103)가 콘텐츠(113)의 정당한 배포자인가를 검증하기 위해 최종 사용자 플레이어 애플리케이션(195)에 의해 이용된다. 최종 사용자 플레이어 애플리케이션(195) 및 클리어링하우스(들)(105)는 전자 디지털 콘텐츠 스토어(들)(103)가 클리어링하우스(105)의 공용 키(621)로 증명서의 기호를 해독함으로써 인증된 배포자임을 검증할 수 있다. 최종 사용자 플레이어 애플리케이션(195)은 설치중에 그 초기화 부분으로서 수신하는 클리어링하우스(105)의 공용 키(621)의 국부 카피를 보존한다.

F. 트랜잭션 보안 컨테이너(640) 포맷

다음의 표는 트랜잭션 SC(들)(640)와 함께 그 BOM 및 키 설명 부문에 포함된 부문들을 보여준다.

부문	BOM		키 설명 부문											
부문 존재	다이제스트	결과명	암호화 알고리즘	Key ID/Enc Key	Sym Key Alg	Sym Key ID								
<table><tr><td>트랜잭션 ID</td></tr><tr><td>최종 사용자(들)의 ID</td></tr><tr><td>최종 사용자(들)의 공용키</td></tr><tr><td>오퍼 SC(s)</td></tr><tr><td>콘텐츠 사용의 선택</td></tr><tr><td>디스플레이를 위한 HTML</td></tr><tr><td>키 설명 부문</td></tr><tr><td>전자 디지털 콘텐츠 스토어(들) 증명서</td></tr></table>	트랜잭션 ID	최종 사용자(들)의 ID	최종 사용자(들)의 공용키	오퍼 SC(s)	콘텐츠 사용의 선택	디스플레이를 위한 HTML	키 설명 부문	전자 디지털 콘텐츠 스토어(들) 증명서	SC 버전					
	트랜잭션 ID													
	최종 사용자(들)의 ID													
	최종 사용자(들)의 공용키													
	오퍼 SC(s)													
	콘텐츠 사용의 선택													
	디스플레이를 위한 HTML													
	키 설명 부문													
	전자 디지털 콘텐츠 스토어(들) 증명서													
	SC ID													
	SC 타입													
	SC 발행자													
일자														
만료일														
다이제스트 알고리즘 ID														
디지털 기호 알고리즘 ID														
Yes	Yes													
Yes	Yes													
Yes	Yes													
Yes	Yes													
콘텐츠 사용의 선택	Yes	Yes												
디스플레이를 위한 HTML	Yes	Yes												
키 설명 부문	Yes	Yes												
전자 디지털 콘텐츠 스토어(들) 증명서	Yes	No												
디지털 기호														

출력 부문	RSA	CH Pub Key
출력 부문	RSA	CH Pub Key

출력 부문	RSA	CH Pub Key
출력 부문	RSA	CH Pub Key

다음은 다른 SC(들)에 대하여 이전에 설명되지 않은 상기 트랜잭션 SC(들)(640)에서 이용되는 용어를 설명한다: • 트랜잭션 ID(535) - 트랜잭션을 유일하게 식별하기 위해 전자 디지털 콘텐츠 스토어(들)(103)에 의해 할당된 ID.

• 최종 사용자(들) ID - 최종 사용자(들)가 구입 선택을 하고 신용 카드 정보를 제공할 때, 전자 디지털 콘텐츠 스토어(들)(103)에 의해 확보된 최종 사용자(들)의 식별.

• 최종 사용자(들)의 공용 키 - 대칭 키(623)를 재암호화하기 위하여 클리어링하우스(들)(105)에 의해 이용된 최종 사용자(들)의 공용 키(661). 최종 사용자(들)의 공용 키(661)는 구매 트랜잭션중에 전자 디지털 콘텐츠 스토어(들)(103)에 전달된다.

• 오퍼 SC(들) - 구매한 콘텐츠(113) 아이템에 대한 오퍼 SC(들)(641).

• 콘텐츠 사용의 선택 - 최종 사용자(들)에 의해 구매한 각 콘텐츠(113) 아이템에 대한 사용 조건의 어레이. 여기에는 각 오퍼 SC(들)(641)에 대한 엔트리가 있다.

• 디스플레이를 위한 HTML - 최종 사용자 플레이어 애플리케이션(195)이 트랜잭션 SC(들)(640)의 수신시 또는 최종 사용자 장치(들)(109)와 클리어링하우스(들)(105)간의 상호작용중에 인터넷 브라우저 윈도우에 디스플레이하는 하나 이상의 HTML 페이지.

최종 사용자 장치(들)(109)가 트랜잭션 SC(들)(640)를 수신하면, 다음의 단계들이 SC(들)의 무결성과 정당성을 입증하기 위해 수행될 수 있다.

1. 클리어링하우스(들)(105)의 공용 키(621)를 이용하여 전자 디지털 콘텐츠 스토어(들)(103)의 무결성을 검증한다. 클리어링하우스(들)(105)의 공용 키(621)는 그 설치 처리중 최종 사용자 플레이어 애플리케이션(195)의 초기화 부문으로 수신된 후, 최종 사용자 장치(들)(109)에 저장된다.

2. 전자 디지털 콘텐츠 스토어(들)(103) 증명서로부터 공용 키를 이용하여 SC(들)의 디지털 기호(643)를 검증한다.

3. SC(들) 부문의 해시를 검증한다.

4. 트랜잭션 SC(들)(640)에 포함된 각 오퍼 SC(들)(641)의 무결성 및 정당성을 입증한다.

G. 오더 보안 컨테이너(650) 포맷

다음의 표는 오더 SC(들)(650)과 함께 그 BOM 및 키 설명 부문에 포함된 부문들을 보여준다. 상기 부문들은 해독화 및 검증 목적으로 클리어링하우스(들)(105)에 정보를 제공하거나, 또는 클리어링하우스(들)(105)에 의해 확인된다. 오퍼 SC(들)(641)로부터의 BOM 및 부문들은 또한 오더 SC(들)(650)에 포함된다. 메타 데이터 SC(들) BOM의 부문 존재 열에서의 일부 스트림은 상기 부문들중 일부가 오더 SC(들)(650)에 포함되지 않음을 표시한다. 메타 데이터 SC(들)(620)로부터의 BOM은 클리어링하우스(들)(105)가 메타 데이터 SC(들)(620) 및 그 부문들의 무결성을 확인할 수 있도록 어떠한 변화 없이 포함된다.

출력 부문	RC4	Enc Sym Key	RSA	CH Pub Key
출력 부문	RC4	Enc Sym key	RSA	CH Pub Key

출력 항목	RCA	Enc Sym key	RSA	CH Pub Key
-------	-----	-------------	-----	------------

메타데이터 SC(s) 80M
부가 및 무지 플드
전자 디지털 콘텐츠
스토어(들) 증명서
증명서(들)

트랜잭션 SC(s) 부문

트랜잭션 ID
최종 사용자(들) ID
최종 사용자(들)의 공용키
오퍼 SC(s)
콘텐츠 사용의 선택
브라우저 윈도우에서 디스플레이하기 위한 HTML
키 설명 부문
전자 디지털 콘텐츠
스토어(들) 증명서

SC(s) 버전	
SC(s) ID	
SC(s) 타입	
SC(s) 발행자	
일자	
만료일	
다이제스트 알고리즘 ID	
디지털 기호 알고리즘 ID	
Yes	Yes
Yes	Yes
Yes	Yes
하나의 오퍼 SC(s)	Yes
Yes	Yes
Yes	Yes
Yes	Yes
Yes	No
디지털 기호	

출력 부문	RSA	CH Pub Key
출력 부문	RSA	CH Pub Key

오퍼 SC(s) BOM		SC(s) 버전		오퍼 SC(s) 부문	
트랜잭션 SC(s) BOM		SC(s) ID			
암호화된 신용 카드 정보		SC(s) 타입			
키 설명 부문		SC(s) 발행자			
		일자			
		만료일			
		다이제스트 알고리즘 ID			
		디지털 기호 알고리즘 ID			
		Yes	Yes		
		Yes	Yes		
		Yes	Yes		
		Yes	Yes		
		디지털 기호			
				출력 부문	
					RSA
					CH Pub Key

다음은 다른 SC(들)에 대하여 이전에 설명되지 않은 상기 오퍼 SC(들)(650)에서 이용된 용어를 설명한다: • 트랜잭션 SC(들) BOM - 원 트랜잭션 SC(들)(640)에서의 BOM. 오퍼 SC(들)(650) BOM에서의 기록은 트랜잭션 SC(들)(640) BOM의 다이제스트를 포함한다.

• 암호화된 신용 카드 정보 - 신용 카드 또는 데빗 카드로 구매에 대한 과금을 하기 위해 이용되는 최종 사용자(들)로부터 선택적 암호화된 정보. 이 정보는 오퍼 SC(들)(641)를 생성한 전자 디지털 콘텐츠 스토어(들)(103)가 고객 빌링(billing)을 관리하지 않을 때 필요하며, 이 경우, 클리어링하우스(들)(105)가 빌링을 관리할 수 있다.

H. 인가 보안 컨테이너(660) 포맷

다음의 표는 인가 SC(들)(660)와 함께 그 BOM에 포함된 부문을 보여준다. 키 설명 부문에서 도시된 바와 같이, 워터마킹 명령, 콘텐츠(113) 및 콘텐츠(113)의 메타 데이터를 해독하기 위해 필요한 대칭 키(623)는 최종 사용자(들)의 공용 키(661)를 이용하여 클리어링하우스(들)(105)에 의해 재암호화된다. 최종 사용자 장치(들)(109)가 인가 SC(들)(660)를 수신하면, 이것은 대칭 키(623)를 해독하고, 이들을 인가 SC(들)(660) 및 콘텐츠 SC(들)(630)로부터 암호화된 부문으로 액세스하기 위해 이용한다.

부문	부문 존재	BOM 다이제스트	키 설명 부문				
			결과명	암호화 알고리즘	Key ID/Enc Key	Sym Key Alg	Sym Key ID
[콘텐츠 URL]			출력 부문	RCA	Enc Sym Key	RSA	EU Pub Key
[메타데이터 URL]			출력 부문	RCA	Enc Sym key	RSA	EU Pub Key
		SC(s) 버전					
		SC(s) ID					
		SC(s) 타입					
		SC(s) 발행자					
		일자					
		만료일					
		다이제스트 알고리즘 ID					
		디지털 기호 알고리즘 ID					
콘텐츠 ID	Yes	Yes					
사용조건	Yes	Yes					
트랜잭션 데이터	Yes	Yes					
위변조 방지	Yes	Yes					
키 설명 부문	Yes	Yes					
증명서(들)	Yes	No					
		디지털 기호					

다음은 다른 SC(들)에 대하여 이전에 설명되지 않은 상기 인가 SC(들)(660)에서 이용된 용어를 설명한다: • EU Pub Key - 데이터를 암호화하기 위해 이용된 최종 사용자의 공용 키(661)를 나타내는 식별자.

• 오더 SC(들)(650) ID -- 오더 SC(들)(650)-BOM으로부터 취해진 SC(들)-ID.

• 증명서 철회 리스트 - 클리어링하우스(들)(105)에 의해 이전에 발행되었지만 더 이상 유효하지 않은 증명서 ID들의 선택적 리스트. 취소 리스트에 포함된 증명서에 의해 검증될 수 있는 기호를 갖는 소정의 SC(들)는 실효된 SC(들)이다. 최종 사용자 플레이어 애플리케이션(195)은 최종 사용자 장치(들)상에 클리어링하우스(105)의 증명서 취소 리스트의 카피를 저장한다. 취소 리스트가 수신될 때마다, 새로운 것이 더 최근의 것이면, 최종 사용자 플레이어 애플리케이션(195)은 그 국부 카피를 대체한다. 취소 리스트는 리스트가 가장 최근의 것인가를 판단하기 위하여 버전 번호 또는 시간 스탬프(또는, 이들 모두)를 포함한다.

1. 콘텐츠 보안 컨테이너 포맷

다음의 표는 콘텐츠 SC(들)(630)와 함께 BOM에 포함된 부문들을 보여준다:

부문	부문 존재	BOM 다이제스트
		SC(s) 버전
		SC(s) ID
		SC(s) 타입
		SC(s) 발행자
		일자
		만료일
		클리어링하우스(들) URL
		다이제스트 알고리즘 ID
		디지털 기호 알고리즘 ID
콘텐츠 ID	Yes	Yes
암호화된 콘텐츠	Yes	Yes
암호화된 메타데이터	Yes	Yes
메타데이터	Yes	Yes
증명서(들)	Yes	No
		다이제스트 기호

다음은 다른 SC(들)에 대하여 이전에 설명되지 않은 상기 콘텐츠 SC(들)(630)에서 이용된 용어를 설명한다:

- 암호화된 콘텐츠 - 대칭 키(623)를 이용하여 콘텐츠 제공자(들)(101)에 의해 암호화된 콘텐츠(113).
- 암호화된 메타 데이터 - 대칭 키(623)를 이용하여 콘텐츠 제공자(들)(101)에 의해 암호화된 콘텐츠(113)와 연관된 메타 데이터.

여기서는 암호화된 부문을 해독하기 위해 필요한 키가 클리어링하우스(들)(105)에서 구축된 인가 SC(들)(660)에 있기 때문에, 콘텐츠 SC(들)(630)에 포함된 키 설명 부문이 없다.

VI. 보안 컨테이너 패킹 및 언패킹

A. 개요

모든 지정된 부문들을 갖는 SC(들)을 생성하기 위한 다중 또는 단일 단계의 처리에서 호출될 수 있는 API(애플리케이션 프로그래밍 인터페이스)를 갖는 32-비트 윈도우즈의 프로그램이다. SC(들) 패커(151, 152, 153)는 콘텐츠 제공자(들)(101), 클리어링하우스(들)(105), 전자 디지털 콘텐츠 스토어(들)(103) 및 SC(들) 패킹을 필요로 하는 다른 사이트들에서 윈도우의 프로그램을 지원하는 다양한 하드웨어 플랫폼이다. BOM 및 필요하다면 키 설명 부문이 생성되어 SC(들)에 포함된다. 패커 API들의 세트는 BOM 및 키 설명 부문의 기록을 생성하며 SC(들)의 부문들을 포함하기 위해 필요한 정보를 호출자가 지정할 수 있도록 한다. 대칭 키(623)와 부문들의 암호화와 함께 다이제스트 및 다이제스트 기호의 계산은 또한 패커에 의해 수행된다. 패커에 의해 지원되는 암호화 및 다이제스트 알고리즘은 패커 코드에 포함되거나, 또는 이들은 외부 인터페이스를 통해 호출된다.

SC(들)를 구축하기 위한 패커와의 인터페이스는 다음의 파라미터들을 입력으로 수신하는 API에 의해 이루어진다.

- 연결된 구성의 버퍼에 대한 포인터. 버퍼에서의 각 구성은 명령을 실행하기 위해 필요한 정보를 갖는 패커로 명령이다. 패커 명령은 연관된 BOM 기록을 갖는 SC(들)에 부문을 추가하는 것과, BOM에 기록을 추가하는 것, 및 키 설명 부문에 기록을 추가하는 것을 포함한다.
- 상술된 버퍼에 포함된 연결된 구성의 수를 나타내는 값.
- BOM 부문의 이름 및 장소.

--- 규정한 플래그 또는 앞으로의 이용을 위해 예약된 플래그인 각 비트를 갖는 값. 다음의 플래그들이 현재 정의된다: ---

- SC(들)의 모든 부문들이 버퍼에서의 모든 구성이 처리된 후에 단일 파일로 함께 묶여야 하는 가에 대한 표시. 부문들을 단일 객체로 묶는 것은 SC(들)를 구축할 때 수행되는 최종 단계이다.
- 디지털 기호가 BOM 부문에서 생략되는 가에 대한 표시. 만약, 상기 플래그가 설정되지 않으면, 디지털 기호는 SC(들)가 단일 객체로 묶이기 직전에 계산된다.

다른 실시예에서, SC(들)를 구축하기 위한 패커와의 인터페이스는 다음의 파라미터들을 입력으로 수신하는 API들에 의해 이루어진다: • 우선, API는 포인터에서, SC(들) BOM 부문에서의 IP 기록, BOM 부문에 이용하기 위한 이름, 추가될 부문들을 찾기 위한 디폴트 장소 및 플래그 값으로 나타나는 SC(들) 설정을 초기화하기 위해 이용되는 정보로 이루어진 구성으로 전달하여 자료의 빌(BOM) 부문을 생성하기 위해 호출된다. 상기 API는 다음의 패커 API들에서 이용되는 SC(들) 관리로 복귀시킨다.

- 패커는 부문이 SC(들)에 추가될 때마다 이용된 API를 갖는다. 상기 API는 이전의 패커 API에 의해 이미 복귀된 SC(들) 관리부, 추가되는 부문에 관한 정보로 이루어진 구성에 대한 포인터 및 플래그 값을 수용한다. 추가될 부문에 관한 정보로는 부문의 이름 및 장소, 부문에 대한 BOM에서 이용하기 위한 이름, 추가될 부문의 타입, 부문을 위한 해시 값, 플래그 등이 있다.
- 부문의 모든 값이 SC(들)에 추가된 후, 패커 API는 BOM 부문을 포함한 모든 부문들을 일반적으로 파일인 단일 SC(들) 객체로 팩하기 위해 호출된다. 상기 API는 이전의 패커 API에 의해 이미 복귀된 SC(들) 관리, 팩된 SC(들)에 이용하기 위한 이름, SC(들)를 부호화하기 위한 정보를 갖는 구성에 대한 포인터 및 플래그 값을 수용한다.

패커를 호출하는 패커 또는 엔티티는 SC(들)를 구축하기 위해 SC(들) 템플릿을 이용할 수 있다. SC(들) 템플릿은 구축될 SC(들)에 필요한 부문 및 기록을 규정하는 정보를 갖는다. 템플릿은 또한 대칭 키(623) 및 암호화된 키를 암호화하기 위해 이용되는 키 참조 및 암호화 방법을 규정할 수 있다.

패커는 SC(들)를 언팩하기 위해 이용된 API를 갖는다. 언패킹 SC(들)는 SC(들)를 취하고, 이것을 그 각 부문들로 분리하는 처리이다. 이때, 패커는 SC(들)로부터 언팩된 암호화된 부문중 일부를 해독하기 위해 호출될 수 있다.

B. 자료의 빌(BOM) 부문

BOM 부문은 SC(들)가 구축될 때 패커에 의해 생성된다. BOM은 SC(들) 및 SC(들)에 포함된 부문에 관한 정보의 기록을 포함한 텍스트 파일이다. BOM 내의 각 기록은 새로운 기록의 개시를 나타내는 새로운 라인을 갖는 단일 라인상에 있다. BOM은 일반적으로 SC(들)의 정당성 및 무결성을 확인하기 위해 이용될 수 있는 디지털 기호 및 각 부문에 대한 다이제스트를 포함한다.

BOM 내의 기록 타입은 다음과 같다: IP IP 기록은 이름의 세트 = SC(들)에 속하는 값의 쌍. 다음의 이름들이 SC(들)의 특정 속성마다 마련된다:

V. 메이저.마이너.고정(major.minor.fix)

V는 SC(들)의 버전을 적절하게 지정한다. 이것은 SC(들)를 생성시킨 SC(들) 명세의 버전 번호이다. 뒤따르는 스트링은 메이저, 마이너, 고정형의 형태로 이루어져야 하며, 여기서 메이저, 마이너 및 고정은 각각 메이저 배포 번호, 마이너 배포 번호 및 고정 레벨이다.

ID 값 ID 속성은 상기 SC(들)를 생성하고 있는 엔티티에 의해 상기 특정한 SC(들)에 할당된 유일 값이다. 이 값의 포맷은 상기 문서의 다음 버전에서 규정된다.

T 값 T 속성은 다음의 것들중 하나인 SC(들)의 타입을 지정한다.

ORD - 오더 SC(들)(650).

OFF - 오퍼 SC(들)(641).

LIC - 인가 SC(들).

TRA - 트랜잭션 SC(들)(640).

MET - 메타 데이터 SC(들)(620).

CON - 콘텐츠 SC(들)(630).

A 값 A 속성은 SC(들)의 저자 또는 발행자를 식별한다. 저자/발행자 동일성은 명확해야 하며 및/또는 클리어링하우스(들)(105)에 등록되어야 한다.

D 값 D 속성은 일자 및 선택적으로 SC(들)가 생성된 시간을 식별한다.

이 값은 연/월/일@시간:분:초.초(시간대)의 소수를 나타내는 yyyy/mm/dd[@hh:mm[:ss]{fsec}][TZ]의 형태로 이루어져야 한다. 이 값의 선택적 부분들은 0 문자로 둘러싸인다.

E 값 E 속성은 일자 및 선택적으로 SC(들)이 만료하는 시간을 식별한다. 이 값은 이전에 규정된 D 속성에서 이용되는 형태와 동일해야 한다. 만료 일/시는 가능한한 클리어링하우스(들)(105)에서의 일/시와 비교되어야 한다.

CCURL 값 CCURL 속성은 클리어링하우스(들)(105)의 URL을 식별한다. 이 값은 유효한 외부 URL의 형태로 이루어져야 한다.

H 값 H 속성은 SC(들)에 포함된 부문들에 대한 메시지 다이제스트를 계산하기 위해 이용된 알고리즘을 식별한다. 일례의 다이제스트 알고리즘은 MD5이다.

D 기록은 부문의 타입, 부문의 이름, 부문의 (선택적)다이제스트 및 부문이 SC(들)에 포함되지 않음의 (선택적)표시를 식별하는 정보를 포함한 데이터 또는 부문 엔트리 기록이다. A-시간 식별자가 부문이 SC(들)에 포함되지 않음을 표시하기 위해 이용된 직후의 번호. 다음의 것들이 부문 기록 또는 데이터의 타입으로 마련된다:

K 부문_이름[다이제스트]키 설명 부문을 지정한다.

W 부문_이름[다이제스트]워터마킹 명령 부문을 지정한다.

C 부문_이름[다이제스트]디지털 기호를 확인하기 위해 이용된 증명서(들)를 지정한다.

T 부문_이름[다이제스트]사용 조건 부문을 지정한다.

YF 부문_이름[다이제스트]오퍼 SC(드)(641)에 대한 템플릿 부문을 지정한다.

YO 부문_이름[다이제스트]오더 SC(들)(650)에 대한 템플릿 부문을 지정한다.

YL 부문_이름[다이제스트]인가 SC(들)(660)에 대한 템플릿 부문을 지정한다.

ID 부문_이름[다이제스트]참조될 콘텐츠(113)의 아이템(들)의 콘텐츠(113) ID(들)를 지정한다.

CH 부문_이름[다이제스트]클리어링하우스(들)(105) 증명서 부문을 지정한다.

SP 부문_이름[다이제스트]전자 디지털 콘텐츠 스토어(들)(103) 증명서 부문을 지정한다.

B 부문_이름[다이제스트]그 부문 또는 상기 SC(들)에 포함된 그 부문들중 일부를 갖는 다른 SC(들)에 대한 BOM을 지정한다.

BP 부문_이름 sc_부문_이름[다이제스트]상기 SC(들)에 단일 부문으로 포함된 다른 SC(들)에 대한 BOM을 지정한다. sc_부문_이름

파라미터는 상기 SC(들)에 포함되며, 상기 BOM 부문이 규정한 SC(들) 부문의 이름이다. 상기 BOM과 동일한 BOM은 또한 sc_부문_명칭 파라미터에 의해 규정된 SC(들)에 포함된다.

D 부문_이름[다이제스트]데이터(또는, 메타 데이터) 부문을 지정한다.

S 기록은 SC(들)의 디지털 기호를 규정하기 위해 이용된 기호 기록이다.

디지털 기호는 다음과 같이 지정된다: S 키_식별자 신호_스트링 기호_알고리즘 S 기록은 기호의 암호화 키, 디지털 기호 비트스트링의 기본 64 인코딩인 기호_스트링, 및 디지털 기호를 생성하기 위한 다이제스트를 암호화하기 위해 이용된 기호 알고리즘을 표시하기 위한 키_식별자를 포함한다.

C. 키 설명 부문

키 설명 부문은 SC(들)의 암호화된 부문들을 해독하기 위해 필요한 암호화 키에 관한 정보를 제공하기 위해 패커에 의해 생성된다. 암호화된 부문들은 구축중인 SC(들)에 포함되거나, 또는 구축중인 SC(들)에 의해 참조되는 다른 SC(들)에 포함될 수 있다. 키 설명 부문은 암호화 키 및 암호화 키가 이용되는 부문들에 관한 정보의 기록을 포함한 텍스트 파일이다. 키 설명 부문에서의 각 기록은 새로운 기록의 개시를 나타내는 새로운 라인을 갖는 단일 라인상에 있다.

다음의 기록 타입은 키 설명 부문 내에서 이용되며, 다음과 같이 규정된다: K 암호화된_부문_이름; 결과_부문_이름; 부문_암호화_알고리즘_식별자; 공용_키_식별자 키_암호화_알고리즘 및 암호화된_대칭_키 K 기록은 상기 SC(들)에 포함되거나, 또는 상기 기록에 의해 참조되는 다른 SC(들)에 포함되는 암호화된 부문을 지정한다. 암호화된_부문_이름은 상기 SC(들)에서의 부문의 이름, 또는 다른 SC(들)에서의 암호화된 부문의 이름을 지시하는 URL이다. 결과_부문_이름은 암호화된 부문에 주어진 이름이다. 부문_암호화_알고리즘은 부문을 암호화하기 위해 이용된 암호화 알고리즘을 표시한다. 공용_키_식별자는 대칭 키(623)를 암호화하기 위해 이용된 키의 식별자이다.

키_암호화_알고리즘_식별자는 대칭 키(623)를 암호화하기 위해 이용된 암호화 알고리즘을 표시한다. 암호화된 대칭 키는 부문을 암호화하기 위해 이용된 암호화된 대칭 키(623) 비트스트링의 기본 64 인코딩이다.

VII. 클리어링하우스(들)(105)

A. 개요

클리어링하우스(들)(105)는 보안 디지털 콘텐츠 전자 배포 시스템(100)의 권리 관리 기능을 맡는다. 클리어링하우스(들)(105) 기능은 전자 디지털 콘텐츠 스토어(들)(103)의 사용화 기능, 콘텐츠(113)의 권리 검증, 구매 트랜잭션 및 관련된 정보의 무결성 및 인증 확인, 최종 사용자 장치(들)(109)로의 콘텐츠 암호화 키 또는 대칭 키(623) 배포, 상기 키들의 배포 추적, 및 전자 디지털 콘텐츠 스토어(들)(103) 및 콘텐츠 제공자(들)(101)에게 트랜잭션 요약을 보고하는 기능들을 포함한다. 콘텐츠 암호화 키는 일반적으로 인증된 전자 디지털 콘텐츠 스토어(들)(103)로부터 구매 트랜잭션에 의해 권리가 획득된 콘텐츠(113)를 로크 해제하기 위해 최종 사용자 장치(들)(109)에 의해 이용된다. 콘텐츠 암호화 키가 최종 사용자 장치(들)(109)에 전송되기 전에, 클리어링하우스(105)는 콘텐츠(113) 및 최종 사용자 장치(들)(109)가 콘텐츠(113)에 대하여 갖는 권리를 판매하고 있는 엔티티의 정당성을 확인하기 위한 검증 처리 전체를 수행한다. 이때 SC 분석 툴(185)이 호출된다. 일부 구성에서, 클리어링하우스(들)(105)는 또한 신용 카드, 인증 및 빌링의 전자 디지털 콘텐츠 스토어(들)(103) 기능을 수행하는 클리어링하우스(들)(105)에서 시스템을 공동 배치시킴으로써 콘텐츠(113) 구매의 금융 결제를 관리할 수 있다. 클리어링하우스(들)(105)는 신용 카드 처리 및 지역 판매세를 관리하기 위해 IC 검증 및 텍스웨어 같은 OEM 패키지를 이용한다.

전자 디지털 콘텐츠 스토어(들) 실시예 보안 디지털 콘텐츠 전자 배포 시스템(100)에서 콘텐츠(113)의 판매자로서 참여하기를 원하는 전자 디지털 콘텐츠 스토어(들)(103)는 보안 디지털 콘텐츠 전자 배포 시스템(100)에 콘텐츠(113)를 제공하는 하나 이상의 디지털 콘텐츠 제공자(들)(101)에게 신청한다. 예컨대, 소니, 타임-워너 등의 음악 레이블 같은 디지털 콘텐츠 레이블로 전자 디지털 콘텐츠 스토어(들)(103)가 그 콘텐츠(113)를 판매할 수 있도록 한 후, 클리어링하우스(들)(105)는 일반적으로 이메일을 통한 신청으로 보안 디지털 콘텐츠 전자 배포 시스템(100)에 부가될 전자 디지털 콘텐츠 스토어(들)(103)와 계약한다. 디지털 콘텐츠 레이블은 전자 디지털 콘텐츠 스토어(들)(103)의 이름, 및 전자 디지털 콘텐츠 스토어(들)(103)에 대한 디지털 증명서를 릴리즈하기 위해 클리어링하우스(들)(105)에 필요한 소정의 다른 정보를 제공한다. 디지털 증명서는 안전한 방식으로 디지털 콘텐츠 레이블에 전송된 후, 디지털 콘텐츠 레이블에 의해 전자 디지털 콘텐츠 스토어(들)(103)로 이동된다. 클리어링하우스(들)(105)는 할당된 디지털 증명서의 데이터 베이스를 관리한다. 각 증명서는 버전 번호, 유일 시리얼 번호, 부호화 알고리즘, 발행자의 이름(예컨대, 클리어링하우스(들)(105)의 이름), 증명서가 유효한 기간, 전자 디지털 콘텐츠 스토어(들)(103)의 이름, 전자 디지털 콘텐츠 스토어(들)(103)의 공용 키, 및 클리어링하우스(들)(105)의 개인 키를 이용하여 부호화된 모든 다른 정보의 해시 코드를 포함한다. 클리어링하우스(들)(105)의 공용 키(621)를 갖는 엔티티들은 증명서를 확인할 수 있는데, 이때 증명서로부터의 공용 키를 이용하여 확인될 수 있는 기호로 SC(들)가 유효한 SC(들)인가를 정확히 확인한다.

전자 디지털 콘텐츠 스토어(들)(103)는 클리어링하우스(들)(105)에 의해 릴리즈된 디지털 증명서 및 디지털 콘텐츠 레이블로부터 SC(들)를 처리하기 위하여 필요한 툴을 수신한 후, 최종 사용자(들)에 의해 구매될 수 있는 콘텐츠(113)의 오퍼링을 개시할 수 있다. 전자 디지털 콘텐츠 스토어(들)(103)는 그 증명서 및 트랜잭션 SC(들)(640)를 포함하고, 그 디지털 기호(643)를 이용하여 SC(들)를 부호화한다. 최종 사용자 장치(들)(109)는, 우선 디지털 증명서 취소 리스트를 검색한 후, 전자 디지털 콘텐츠 스토어(들)(103)에 대한 디지털 증명서에서의 정보를 검증하기 위해 클리어링하우스(들)(105)의 공용 키(621)를 이용함으로써, 전자 디지털 콘텐츠 스토어(들)(103)가 보안 디지털 콘텐츠 전자 배포 시스템(100)에서의 콘텐츠(113)의 정당한 배포자인가를 검증한다. 디지털 증명서 취소

리스트는 클리어링하우스(들)(105)에 의해 관리된다. 취소 리스트는 클리어링하우스(들)에 의해 생성된 인가 SC(들)(660)에서의 부문들중 하나로서 포함될 수 있다. 최종 사용자 장치(들)(109)는 최종 사용자 장치(들)(109)상의 취소 리스트의 카피를 보존하여, 이들이 전자 디지털 콘텐츠 스토어(들)(103)의 디지털 증명서 확인 부분으로 이용될 수 있도록 한다.

최종 사용자 장치(들)(109)가 인가 SC(들)(660)를 수신할 때마다, 새로운 취소 리스트가 포함되었는가를 판단하여, 만약 있다면, 최종 사용자 장치(들)(109)상의 국부적 취소 리스트가 갱신된다.

B. 권리 관리 처리

오더 SC(들) 분석클리어링하우스(들)(105)는, 최종 사용자(들)가 전자 디지털 콘텐츠 스토어(들)(103)로부터 오퍼 SC(들)(641)를 포함한 트랜잭션 SC(들)(640)를 수신한 후, 최종 사용자(들)로부터 오더 SC(들)(650)를 수신한다. 오더 SC(들)(650)는 콘텐츠(113)와 그 이용과 관련된 정보, 콘텐츠(113)를 판매하는 전자 디지털 콘텐츠 스토어(들)(103)에 관한 정보, 및 콘텐츠(113)를 구매하는 최종 사용자(들)에 관한 정보를 포함한 부문들로 구성된다. 클리어링하우스(들)(105)는 오더 SC(들)(650)에서의 정보 처리를 개시하기 전에, 우선 SC(들)가 실제 정당한 것이며, 이것을 포함한 데이터가 어떤 방식으로든 훼손되지 않았음을 보증하기 위하여 소정의 처리를 수행한다.

확인클리어링하우스(들)(105)는 디지털 기호를 검증함으로써, 오더 SC(들)(650)의 확인을 개시하고, 이어서 클리어링하우스(들)(105)는 오더 SC(들)(650) 부문의 무결성을 검증한다. 디지털 기호를 확인하기 위하여, 우선 클리어링하우스(들)(105)는 부호화되었을 때 포함되는 부호화 엔티티(부호화 엔티티는 콘텐츠 제공자(들)(101), 전자 디지털 콘텐츠 스토어(들)(103), 최종 사용자 장치(들)(109) 또는 이들의 소정의 조합일 수 있음)의 공용 키(661)를 이용하여 기호로 된 콘텐츠(631)를 자체적으로 해독한다. 이후, 클리어링하우스(들)(105)는 SC(들)의 연결된 부문 다이제스트들의 다이제스트를 계산하고, 이것을 디지털 기호의 암호화된 콘텐츠(113)와 비교한다. 만약, 두 개의 값들이 일치하면, 디지털 기호는 유효한 것이다. 각 부문의 무결성을 검증하기 위하여, 클리어링하우스(들)(105)는 부문의 다이제스트를 비교하고, 이것을 BOM에서의 다이제스트 값에 비교한다. 클리어링하우스(들)(105)는 오더 SC(들)(650) 내에 포함된 오퍼 SC(들)(641) 부문들과 메타 데이터에 대한 디지털 기호 및 부문 무결성을 검증하기 위하여 동일한 처리를 지속한다.

오퍼 SC(들)(641) 디지털 기호 및 트랜잭션의 확인 처리는 또한 전자 디지털 콘텐츠 스토어(들)(103)가 보안 디지털 콘텐츠 전자 배포 시스템(100)에 의해 인증되었음을 간접적으로 검증한다. 이것은 클리어링하우스(들)(105)가 증명서의 발행자인 사실에 기초한다. 또한, 클리어링하우스(들)(105)는, SC(들)를 부호화한 엔티티가 연관된 개인 키의 소유권을 갖을 때만, 전자 디지털 콘텐츠 스토어(들)(103)로부터의 공용 키를 이용하여 오퍼 SC(들)(641) 및 트랜잭션 SC(들)(640)의 디지털 기호를 확실하게 검증할 수 있다. 전자 디지털 콘텐츠 스토어(들)(103)만이 개인 키의 소유권을 갖는다. 클리어링하우스(들)(105)가 전자 디지털 콘텐츠 스토어(들)(103)의 국부적 데이터베이스를 갖을 필요가 없음을 알 수 있는데, 그 이유는, 스토어가 트랜잭션 SC(들)(640) 및 오퍼 SC(들)(641)의 공용 키를 부호화하기 위하여 클리어링하우스 공용 키를 이용하기 때문이다.

다음에, 최종 사용자(들)가 구매중인 콘텐츠(113)의 스토어 사용 조건(519)이 메타 데이터 SC(들)(620)에 설정되어 있는 제한 내에서 과해짐을 보장하기 위하여 클리어링하우스(들)(105)에 의해 확인된다. 메타 데이터 SC(들)(620)가 오더 SC(들)(650) 내에 포함됨을 상기한다.

키 처리암호화된 대칭 키(623) 및 워터마킹 명령의 처리는, 오더 SC(들)(650)의 정당성 및 무결성 검색, 전자 디지털 콘텐츠 스토어(들)(103)의 확인, 및 스토어 사용 조건(519)의 확인이 성공적으로 완료된 후, 클리어링하우스(들)(105)에 의해 수행된다. 오더 SC(들)(650)의 메타 데이터 SC(들)(620) 부문은 일반적으로 클리어링하우스(들)(105)의 공용 키(621)를 이용하여 암호화된 키 설명 부문에 위치한 여러 개의 대칭 키(623)를 갖는다. 대칭 키(623)의 암호화는 메타 데이터 SC(들)(620)가 생성될 때 콘텐츠 제공자(들)(101)에 의해 이루어진다.

하나의 대칭 키(623)가 워터마킹 명령을 해독하기 위해 이용되며, 다른 대칭 키가 콘텐츠(113) 및 소정의 암호화된 메타 데이터를 해독하기 위해 이용된다. 콘텐츠(113)는 하나의 곡 또는 CD상의 곡의 전체 모음을 나타낼 수 있기 때문에, 다른 대칭 키(623)가 각 곡마다 이용될 수 있다. 워터마킹 명령은 오더 SC(들)(650) 내의 메타 데이터 SC(들)(620) 부분에 포함된다. 콘텐츠(113) 및 암호화된 메타 데이터는 콘텐츠 호스팅 사이트(들)(111)에서의 콘텐츠 SC(들)(630)에 있다. 콘텐츠 SC(들)(630) 내에 있는 암호화된 콘텐츠(113)의 URL 및 부문명과 메타 데이터 부문들은 오더 SC(들)(650)의 메타 데이터 SC(들)(620) 부분의 키 설명 부문에 포함된다. 클리어링하우스(들)(105)는 대칭 키(623)를 해독하기 위하여 그 개인 키를 이용하고, 이어서 이들 각각을 최종 사용자 장치(들)(109)의 공용 키(661)를 이용하여 암호화한다. 최종 사용자 장치(들)(109)의 공용 키(661)는 오더 SC(들)(650)로부터 검색된다. 새로운 암호화된 대칭 키(623)는 클리어링하우스(들)(105)가 최종 사용자 장치(들)(109)로 복귀하는 인가 SC(들)(660)의 키 설명 부문에 포함된다.

대칭 키(623)의 처리 기간중, 클리어링하우스(들)(105)는 워터마킹 명령에 수정을 가하고자 할 수 있다. 이 경우, 클리어링하우스(들)(105)가 대칭 키(623)를 해독한 후, 워터마킹 명령이 수정되어 재암호화된다. 새로운 워터마킹 명령이 최종 사용자 장치(들)(109)로 복귀된 인가 SC(들)(660) 내의 부문들중 하나로서 포함된다.

오더 SC(들)(650)의 모든 처리가 성공적이면, 클리어링하우스(들)(105)는 인가 SC(들)(660)를 최종 사용자 장치(들)(109)로 되돌린다. 최종 사용자 장치(들)(109)는 콘텐츠 SC(들)(630)를 다운로드하고 암호화된 콘텐츠(113) 및 메타 데이터에 액세스하기 위하여 인가 SC(들)(660) 정보를 이용한다. 워터마킹 명령은 또한 최종 사용자 장치(들)(109)에 의해 실행된다.

클리어링하우스(들)(105)가 오더 SC(들)(650)를 성공적으로 처리할 수 없을 때, HTML 페이지는 최종 사용자 장치(들)(109)로 복귀되어 인터넷 브라우저 윈도우에 디스플레이된다. HTML 페이지는 클리어링하우스(들)(105)가 트랜잭션을 처리할 수 없는 이유를 표

시한다.

다른 실시예에서, 사용자가 판매를 위해 설정된 릴리즈 일자 전에 콘텐츠(113)의 카피를 구매할 경우, 인가(들) SC(660)는 대칭 키(623) 없이 복귀된다. 인가(들) SC(660)는 대칭 키를 수신하기 위한 릴리즈 일자 또는 그 후에 클리어링하우스(들)(105)로 복귀된다. 일례로서, 콘텐츠 제공자(들)(101)는 고객이 곡을 다운로드 받을 수 있도록 된 곡에 대한 릴리즈 일자 전에 사용자가 새로운 곡을 다운로드 받을 수 있도록 하며, 콘텐츠 제공자(들)(101)에 의해 설정된 일자 전에 곡을 플레이하기 위한 준비를 할 수 있다. 이로서, 릴리즈 일자에서 대역폭 및 다운로드 시간에 대한 콘텐츠 없이도 릴리즈 일자에서 콘텐츠(113)의 열기를 즉시 허용할 수 있다.

C. 국가 지정 파라미터

선택적으로, 클리어링하우스(들)(105)는 최종 사용자 장치(들)(109)의 도메인명 및 가능하다면 언제나 최종 사용자(들)의 국가 장소를 결정하기 위하여 신용 카드 빌링 어드레스를 이용한다. 최종 사용자(들)가 거주하는 국가에서의 콘텐츠(113)의 판매를 위한 소정의 제한이 있다면, 이때 클리어링하우스(들)(105)는 처리된 트랜잭션이 인가 SC(들)(660)를 최종 사용자 장치(들)(109)에 전송하기 전에 소정의 상기 제한들을 위반하지 않음을 보증한다. 전자 디지털 콘텐츠 스토어(들)(103)는 또한 클리어링하우스(들)(105)에서와 같은 검색을 수행함으로써 여러 개의 국가들로의 콘텐츠(113)의 배포 관리에 참여하게 된다. 클리어링하우스(들)(105)는 전자 디지털 콘텐츠 스토어(들)(103)가 콘텐츠 제공자(들)(101)에 의해 설정된 국가 지정 규칙을 무시하는 경우에 이들이 할 수 있는 어떠한 검색이라도 수행한다.

D. 감사 로그 및 추적

클리어링하우스(들)(105)는 콘텐츠(113)가 트랜잭션을 구매하고 요구 트랜잭션을 보고하는 동안 수행되는 각 동작중에 정보의 감사 로그(150)를 관리한다. 정보는 보안 디지털 콘텐츠 전자 배포 시스템(100)의 감사, 보고의 발생 및 데이터 마이닝 같은 다양한 목적을 위해 이용될 수 있다.

클리어링하우스(들)(105)는 또한 전자 디지털 콘텐츠 스토어(들)(103)에 대한 빌링 보조 시스템(182)에서의 회계 조정을 관리한다. 전자 디지털 콘텐츠 스토어(들)(103)에 대한 가격 구조는 디지털 콘텐츠 레이블에 의해 클리어링하우스(들)(105)에 제공된다. 상기 정보는 전자 디지털 콘텐츠 스토어(들)(103)에 부여될 필요가 있는 회계, 결손 제한, 양의 할인 및 현재의 특별 상품을 포함할 수 있다. 클리어링하우스(들)(105)는 전자 디지털 콘텐츠 스토어(들)의 대차 대조를 추적하고, 이들이 콘텐츠 제공자(들)(101)에 의해 설정된 결손 제한을 넘지 않음을 보증하기 위하여 가격 정보를 이용한다.

다음의 동작들이 일반적으로 클리어링하우스(들)(105)에 의해 로그된다: • 인가 SC(들)(660)에 대한 최종 사용자 장치(들)(109)의 요구 • 클리어링하우스(들)(105)가 빌링을 관리할 때의 신용 카드 인증 번호 • 최종 사용자 장치(들)(109)로의 인가 SC(들)(660)의 분산 • 보고에 대한 요구 • 콘텐츠 SC(들)(630) 및 인가 SC(들)(660)가 수신되어 확인된 최종 사용자(들)로부터의 통지다음의 정보가 일반적으로 인가 SC(들)(660)에 대한 클리어링하우스(들)(105)에 의해 로그된다: • 요구 일자 및 시간 • 구매 트랜잭션 일자 및 시간 • 구매된 아이템의 콘텐츠 ID • 콘텐츠 제공자(들)(101)의 식별 • 스토어 사용 조건(519) • 워터마킹 명령 수정 • 전자 디지털 콘텐츠 스토어(들)(103)에 의해 부가된 트랜잭션 ID(535) • 전자 디지털 콘텐츠 스토어(들)(103)의 식별 • 최종 사용자 장치(들)(109)의 식별 • (클리어링하우스(들)(105)가 빌링을 관리하는 경우에)최종 사용자(들) 신용 카드 정보다음의 정보는 일반적으로 최종 사용자의 신용 카드 정보에 대한 클리어링하우스(들)(105)에 의해 로그된다: • 요구 일자 및 시간 • 신용 카드에 과금된 액수 • 구매된 아이템의 콘텐츠 ID • 전자 디지털 콘텐츠 스토어(들)(103)에 의해 부가된 트랜잭션 ID(535) • 전자 디지털 콘텐츠 스토어(들)(103)의 식별 • 최종 사용자(들)의 식별 • 최종 사용자(들) 신용 카드 정보 • 신용 카드의 클리어기로부터 수신된 인증 번호다음의 정보는 일반적으로 인가 SC(들)(660)가 최종 사용자 장치(들)(109)에 전송될 때 클리어링하우스(들)(105)에 의해 로그된다: • 요구 일자 및 시간 • 구매된 아이템의 콘텐츠 ID • 콘텐츠 제공자(들)(101)의 식별 • 사용 조건(517) • 전자 디지털 콘텐츠 스토어(들)(103)에 의해 부가된 트랜잭션 ID(535) • 전자 디지털 콘텐츠 스토어(들)(103)의 식별 • 최종 사용자(들)의 식별다음의 정보는 일반적으로 보고 요구가 이루어질 때 로드된다: • 요구 일자 및 시간 • 보고가 전송된 일자 및 시간 • 요구된 보고의 타입 • 보고를 발생하기 위해 이용된 파라미터들 • 보고를 요구하는 엔티티의 식별자E. 결과의 보고

보고는 최종 사용자(들) 구매 트랜잭션중 로그된 클리어링하우스(들)(105)에서의 정보를 이용하여 클리어링하우스(들)(105)에 의해 발생된다. 콘텐츠 제공자(들)(101) 및 전자 디지털 콘텐츠 스토어(들)(103)는 지불 검증 인터페이스(183)를 통해 클리어링하우스(들)(105)로부터 트랜잭션 보고를 요청하여, 이들이 자체의 트랜잭션 데이터베이스와 클리어링하우스(들)(105)에 의해 로그된 정보와 일치화시키도록 한다. 클리어링하우스(들)(105)는 또한 콘텐츠 제공자(들)(101) 및 전자 디지털 콘텐츠 스토어(들)(103)에 주기적인 보고를 제공할 수 있다.

클리어링하우스(들)(105)는 콘텐츠 제공자(들)(101) 및 전자 디지털 콘텐츠 스토어(들)(103)가 보고를 요구하여 수신할 수 있도록 하는 보안 전자 인터페이스를 규정한다. 보고 요구 SC(들)는 요구를 개시하는 엔티티에 클리어링하우스(들)(105)에 의해 할당된 증명서를 포함한다. 클리어링하우스(들)(105)는 인증된 엔티티로부터 발생된 요구를 검증하기 위하여 증명서 및 SC의 디지털 기호를 이용한다. 요구는 또한 보고의 범위를 규정하는 시간 기간 같은 파라미터를 포함한다. 클리어링하우스(들)(105)는 요구자가 그들이 갖을 수 있도록 허용된 정보만을 수신할 수 있도록 보증하기 위해 요구 파라미터들을 확인한다.

만약, 보고 요구 SC(들)가 정당하며 유효한 것이라고 클리어링하우스(들)(105)가 판단하면, 이때 클리어링하우스(들)(105)는 보고를 발생하고, 이것을 요구를 개시한 엔티티에 전송될 보고 SC(들)에 찍시킨다. 일부 보고들은 규정된 시간 간격으로 자동적으로 발생되어 클리어링하우스(들)(105)에 저장되어, 이들이 요구가 수신될 때 바로 전송될 수 있도록 한다. 보고에 포함된 데이터의 포맷은 상기 문서의 다음 버전에서 규정된다.

F. 빌링 및 지불 검증

콘텐츠(113)의 빌링은 클리어링하우스(들)(105) 또는 전자 디지털 콘텐츠 스토어(들)(103)에 의해 관리될 수 있다. 클리어링하우스(들)(105)가 전자 콘텐츠(113)의 빌링을 관리하는 경우, 전자 디지털 콘텐츠 스토어(들)(103)는 최종 사용자(들)의 오더를 전자 제품, 및 적용될 수 있다면 물리적 제품으로 분리한다. 이때, 전자 디지털 콘텐츠 스토어(들)(103)는 인증에 필요한 총량 및 최종 사용자(들)의 빌링 정보를 포함한 트랜잭션의 클리어링하우스(들)(105)에 통지한다. 클리어링하우스(들)(105)는 최종 사용자(들)의 신용 카드를 인증하고, 통지를 다시 전자 디지털 콘텐츠 스토어(들)(103)로 복귀시킨다. 클리어링하우스(들)(105)가 최종 사용자(들)의 신용 카드를 인증함과 동시에, 전자 디지털 콘텐츠 스토어(들)(103)는 구매한 소정의 물리적 제품에 대하여 최종 사용자(들)의 신용 카드에 과금시킬 수 있다. 각 전자 아이템이 최종 사용자 장치(들)(109)에 의해 다운로드된 후, 클리어링하우스(들)(105)는 최종 사용자(들)의 신용 카드가 과금될 수 있도록 통지받는다. 이것은 콘텐츠(113)가 최종 사용자 장치(들)(109)에서 이용될 수 있기 전에, 최종 사용자 장치(들)(109)에 의해 최종 단계로서 발생한다.

전자 디지털 콘텐츠 스토어(들)(103)가 전자 콘텐츠(113)의 빌링을 관리하는 경우에, 클리어링하우스(들)(105)는 최종 사용자 장치(들)(109)가 오더 SC(들)(650)를 클리어링하우스(들)(105)에 전송할 때까지 트랜잭션에 관하여 통지받는다. 클리어링하우스(들)(105)는 또한 각 전자 아이템이 다운로드된 후, 최종 사용자 장치(들)(109)에 통지된다. 클리어링하우스(들)(105)가 통지받으면, 이것을 전자 디지털 콘텐츠 스토어(들)(103)에 통지를 전송하여, 전자 디지털 콘텐츠 스토어(들)(103)가 최종 사용자(들)의 신용 카드에 과금할 수 있도록 한다.

G. 재전송

보안 디지털 콘텐츠 전자 배포 시스템(100)은 콘텐츠(113)의 재전송을 관리하는 기능을 제공한다. 이것은 일반적으로 고객 서비스 인터페이스(184)에 의해 수행된다. 전자 디지털 콘텐츠 스토어(들)(103)는 최종 사용자(들)가 재전송을 개시하기 위하여 거칠 수 있는 사용자 인터페이스를 제공한다. 최종 사용자(들)는 콘텐츠(113) 아이템이 콘텐츠(113)의 재전송을 요구하기 위하여 구매한 전자 디지털 콘텐츠 스토어(들)(103) 사이트로 진행한다.

콘텐츠(113)의 재전송은, 콘텐츠(113)가 다운로드될 수 없거나 또는 다운로드된 콘텐츠(113)가 이용될 수 없기 때문에, 최종 사용자(들)가 이미 구매한 콘텐츠(113) 아이템의 새로운 카피를 요구할 때 수행된다. 전자 디지털 콘텐츠 스토어(들)(103)는 최종 사용자(들)가 콘텐츠(113)의 재전송을 수행하기 위한 권리를 갖고 있는가의 여부를 판단한다. 최종 사용자(들)가 재전송에 대한 권리를 갖고 있다면, 이때 전자 디지털 콘텐츠 스토어(들)(103)는 전송된 콘텐츠(113) 아이템(들)의 오퍼 SC(들)(641)를 포함한 트랜잭션 SC(들)(640)를 구축한다. 트랜잭션 SC(들)(640)는 최종 사용자 장치(들)(109)에 전송되고, 구매 트랜잭션에 관하여 동일한 단계들이 최종 사용자(들)에 의해 수행된다. 최종 사용자 장치(들)(109)가 재전송용 콘텐츠(113) 아이템(들)에 대한 키 라이브러리에 스크램블된 키(들)를 갖는다면, 이때 트랜잭션 SC(들)(640)는 스크램블된 키(들)를 삭제하기 위하여 최종 사용자 장치(들)(109)에 명령하는 정보를 포함한다.

클리어링하우스(들)(105)가 콘텐츠(113) 구매의 금융 결제를 관리하는 경우에, 전자 디지털 콘텐츠 스토어(들)(103)는 오더 SC(들)(650)에서의 클리어링하우스(들)(105)로 향하여 전달되는 트랜잭션 SC(들) 내의 플래그를 포함한다. 클리어링하우스(들)(105)는 오더 SC(들)(650)에서의 플래그를 해석하고, 콘텐츠(113)의 구매에 대하여 최종 사용자(들)에게 과금하지 않고 트랜잭션을 처리한다.

VIII. 콘텐츠 제공자

A. 개요

보안 디지털 콘텐츠 전자 배포 시스템(100)에서의 콘텐츠 제공자(들)는 콘텐츠(113)에 대한 권리를 소유한 엔티티 또는 디지털 콘텐츠 레이블이다. 콘텐츠 제공자(들)(101)의 역할은 배포를 위한 콘텐츠(113)를 준비하여, 전자 디지털 콘텐츠 스토어(들)(103) 또는 콘텐츠(113)의 다운로드 가능한 전자 버전의 소매자에게 이용가능한 콘텐츠(113)에 관한 정보를 작성하는 것이다. 콘텐츠 제공자(들)(101)에게 최대한의 보안 및 권리 제어를 제공하기 위하여, 일련의 툴들이, 콘텐츠가 콘텐츠 제공자(들)(101)의 도메인을 넘겨 놓았을 때 보안되어, 비인증된 대상에 의해 노출되거나 액세스될 수 없도록, 콘텐츠 제공자(들)(101)가 콘텐츠(113)를 준비하여 안전하게 그들의 프레미스(premise)에서의 SC(들)로 패키징할 수 있도록 제공된다. 이로써 콘텐츠(113)가 해커나 비인증된 대상에게 노출될 우려 없이 인터넷 같은 비-보안 네트워크를 통해 자유롭게 배포될 수 있게 된다.

콘텐츠 제공자(들)(101)에 대한 툴의 최종 목적은, 곡 또는 일련의 곡들 같은 콘텐츠(113)를 준비하여 콘텐츠 SC(들)(630)로 패키징하며, 곡을 설명하는 정보, 곡의 승인된 이용(콘텐츠 사용 조건(517)) 및 곡에 대한 프로모션형 정보를 메타 데이터 SC(들)(620)로 패키징하기 위한 것이다. 이를 구현하기 위하여, 다음의 툴 세트가 제공된다:

- 워크 플로우 관리자(154) - 처리 활동을 스케줄하고, 처리의 필요한 동기를 관리한다.
- 콘텐츠 처리 툴(155) - 워터마킹, 전처리(오디오의 예에서는, 소정의 필요한 등화, 동적 조정 또는 재샘플링), 인코딩 및 압축을 포함한 콘텐츠(113) 파일 준비를 제어하기 위한 툴의 집합.
- 메타 데이터 및 엔트리 툴(161) - 조작자 상호작용을 통해서 콘텐츠 제공자(들) 및/또는 제 3자 데이터 베이스 또는 데이터 수입 파일들로부터 콘텐츠(113) 설명 정보를 수집하고, 콘텐츠 사용 조건(517)을 지정하기 위한 수단을 제공하기 위하여 이용된다. 또한, CDS 또는 DDP에 대한 디지털 오디오 콘텐츠 같은 콘텐츠를 입수하거나 추출하기 위한 인터페이스가 제공된다. 품질 제어 툴은 준비된 콘텐츠 및 메타 데이터를 미리 볼 수 있다. 다른 처리를 위한 콘텐츠의 재전송 및 메타 데이터에 필요한 소정의 수정이 수행될 수 있다.

- SC(들) 팩커 툴(152) - 모든 콘텐츠(113) 및 정보를 암호화하여 패키징하고, SC(들)로 팩하기 위해 SC(들) 팩커를 호출한다.
- 콘텐츠 분산 툴(도시되지 않음) - 콘텐츠 호스팅 사이트(들)(111) 및 전자 디지털 콘텐츠 스토어(들)(103) 같은 지정된 배포 센터로 SC(들)를 분산시킴.
- 콘텐츠 프로모션형 웹 사이트(156) - 인증된 전자 디지털 콘텐츠 스토어(들)(103)에 의한 다운로드를 위해 메타 데이터 SC(들)(620) 및 선택적으로 부가 프로모션형 자료를 기억한다.

B. 워크 플로우 관리자(154)

상기 툴의 목적은 콘텐츠(113) 처리 작용을 스케줄, 추적 및 관리하기 위한 것이다. 상기 애플리케이션은 콘텐츠 제공자(들)(101)의 인트라넷 또는 엑스트라넷에서 원격인 장소로부터의 상태 검색 및 콘텐츠(113)의 스케줄링 허용과 함께 다중 사용자 액세스를 가능하게 한다. 이러한 디자인은 또한 다수의 개체가 다중 피스의 콘텐츠(113)에서 병렬로 작업할 수 있고, 다른 개체들이 특정한 역할을 할당받을 수 있는 경우에 협조하여 처리할 수 있도록 하며, 상기 개체들은 전세제로 확산될 수 있다.

이하, 도 7에 대응하는 워크 플로우 관리자(154)의 주요한 처리들의 블록도인 도 8을 참조한다. 도 8에서의 주요한 처리들은 상기 섹션에서 설명된 툴에 의해 제공된 콘텐츠(113) 처리 기능을 요약한다. 워크 플로우 관리자(154)는 상기 처리에 대한 작업(job)을 제공해야 하고, 그 현재 처리의 완료시 다음에 필요한 처리에 대한 작업을 전달한다. 이것은 각 처리 툴이 호출하는 일련의 애플리케이션 프로그래밍 인터페이스(API)를 통해 구현된다:

- 처리를 위해 다음 작업을 검색한다
 - 처리의 성공적인 완료를 표시한다
 - 처리의 불완전한 완료 및 실패 이유를 표시한다
 - (종속적인 처리의 부분적인 완료만을 필요로 하는 처리의 개시를 허용하기 위하여) 처리의 중간 상태를 제공한다
 - 지시된 처리에 이용될 수 있는 저작물에 코멘트를 부가한다
- 워크 플로우 관리자(154)는 또한 사용자 인터페이스를 갖고, 일련의 워크 플로우 관리자 사용자 인터페이스(700)는 다음의 기능들을 제공하는 도 7에 예시된다.

- 디폴트 값의 명세 및 여러 단계의 처리중 할당 및 수행되는 조건을 제공하는 구성 패널
 - 워크 플로우 규칙의 개별화 및 자동화된 처리 흐름
 - 작업 스케줄링
 - 상태 질의 및 보고
 - 연관된 작업에 대한 코멘트 또는 명령을 하나 이상의 처리에 부가한다
 - 작업 관리 (즉, 일시 정지, 해제, 제거, 우선 순위 변경(처리 순서))
- 각 처리는 워크 플로우 관리자(154)에 의해 관리되는 것과 연관된 큐(queue)를 갖는다. 워크 플로우 관리자(154)로부터의 모든 처리 요구 작업은, 워크 플로우 관리자(154)에서 현재 연관된 큐에 어떠한 작업도 없다면 대기 상태에서의 처리(들)를 일시 정지하거나 또는 그 각 처리를 수행하기 위해 필요한 작업에 관한 모든 정보를 처리하기 위하여 되돌아가게 된다. 만약, 처리가 대기 상태에서 일시 정지되면, 작업이 워크 플로우 관리자(154)에 의해 그 큐에 배치될 때 처리를 재개한다.

워크 플로우 관리자(154)는 또한 규정된 규칙 세트에 기초하여 처리의 흐름 또는 오더를 관리한다. 상기 규칙은 특별한 처리 조건을 갖거나 특정한 디폴트 규칙을 구성한다면, 콘텐츠 제공자(들)(101)에 의해 개별화된다. 처리가 그 할당된 태스크의 완료를 보고하면, 이러한 상태를 워크 플로우 관리자(154)에게 통지하고, 워크 플로우 관리자(154)는 어떠한 큐 작업이 규정된 규칙에 기초하여 다음에 배치되는가를 결정한다.

특별한 관리 명령 또는 통지를 표시하는 코멘트는 또한 워크 플로우 관리자 사용자 인터페이스(700) 또는 처리기 인터페이스를 통해 수동으로, 또는 프로그래밍 API를 통해 소정의 처리 단계들에서의 저작물에 첨부될 수 있다.

워크 플로우 관리자(154)에서의 처리는 양호한 실시예에서 자바로 실시될 수 있지만, C/C++, 어셈블러 등의 다른 프로그래밍 언어들이 이용될 수 있다. 워크 플로우 관리자(154)에 대하여 이하에 설명되는 처리가 다양한 하드웨어 및 소프트웨어 플랫폼에서 실행될 수 있음을 이해하여야 한다. 완전한 시스템 또는 그것을 구성하는 처리의 일부로서의 워크 플로우 관리자(154)는 웹 또는 플로피 디스크, CD ROM 및 이동 하드디스크 드라이브 같은 전자 배포물을 포함하지만 이에 한정되지 않는 컴퓨터 판독가능 매체에서의 애플리케이션 프로그램으로 배포될 수 있다.

이하, 도 7에 대응하는 워크 플로우 관리자(154)의 주요한 처리들의 블록도인 도 8을 참조한다. 다음의 섹션들은 각 처리를 요약한 것이며, 각 처리 필요한 정보 및 활동을 설명한다.

1. 저작물 대기 활동/정보 처리(801)

일단, 처리에 필요한 모든 정보가 이용될 수 있고, 작업이 이미 모든 종속 처리를 성공적으로 완료하면, 작업은 특정한 처리 큐에 배치된다. 정보의 부재 또는 다른 처리의 방지 실패로 인해 현재 처리를 위해 이용될 수 없는 작업을 홀드하기 위해 이용된 워크 플로우 관리자(154)에는 특별한 큐가 존재한다. 상기 작업들은 저작물 대기 활동/정보 처리(801) 큐에 배치된다. 상기 큐에서의 각 작업은 활동 또는 정보를 표시하기 위한 상태와 연관되어, 상기 작업에서 작업된 최종 처리 및, 일단 정보 부재 또는 부가가 제공되거나 또는 필요한 활동이 성공적으로 완료되면 상기 작업이 큐되는 다음 처리(들)를 대기한다.

소정의 처리의 완료시 워크 플로우 관리자(154)가 상기 큐를 검사할 수 있고, 상기 큐에서의 소정의 작업이 상기 처리(활동)의 종료 또는 상기 처리에 의해 제공된 정보를 대기하고 있는가를 판단한다. 만약, 그렇다면, 작업은 적절한 처리 큐를 위해 큐된다.

2. 새로운 콘텐츠 요구 처리(802)

콘텐츠 제공자(들)(101)는 상기 저작물(예컨대, 저작물은 곡 또는 곡의 집합일 수 있음)이 전자적으로 판매 및 배달되기를 원하는가

를 판단한다. 워크 플로우 관리자(154)의 초기 기능은 조작자가 상기 저작물을 식별하여 이들을 새로운 콘텐츠 요구 처리(802)의 큐에 배치하도록 하는 것이다. 콘텐츠 제공자(들)(101)는 어떤 정보가 저작물 선택 인터페이스에서 프롬프트되는 가를 구성 옵션을 통해 지정할 수 있다. 유일하게 저작물을 식별하기 위해 충분한 정보가 기입된다. 선택적으로, 부가 필드가 메타 데이터 취득과 병행하여 오디오 처리 단계를 개시하기 위해 필요한 정보의 수동 엔트리를 요구하기 위해 포함될 수 있다. 만약, 수동으로 제공되지 않으면, 상기 정보는 자동 메타 데이터 취득 처리(803)에서와 같은 메타 데이터 처리의 제 1 단계에서 얻어진 콘텐츠 제공자(들)의 데이터베이스(160)로부터, 또는 디폴트 구성 설정으로부터 선택적으로 검색될 수 있다. 콘텐츠 제공자(들)의 데이터베이스(160)에서의 콘텐츠(113)의 제작 및 기능이 콘텐츠 선택 처리를 결정한다.

만약, 콘텐츠 제공자(들)(101)의 데이터베이스(160)로의 질의를 수행하기 위해 요구되는 필요한 정보가 지정되면, 작업은 자동 메타 데이터 취득 처리(803)에 의해 처리된다. 음악의 예에서, 오디오 처리를 위해 저작물을 적절하게 스케줄링하기 위하여, 저작물의 장르 및 소망하는 압축 레벨이 오디오 PCM 또는 WAV 파일명(들)과 함께 지정된다. 상기 정보는 저작물 선택 처리 부분으로 기입되거나, 또는 개별화된 질의 인터페이스 또는 웹 브라우저 기능을 통해 선택될 수 있다. 상기 정보의 명세는 저작물이 콘텐츠 처리를 위해 스케줄되도록 한다.

저작물 선택 사용자 인터페이스는 저작물이 처리를 위해 릴리즈될 수 있는 가의 여부, 또는 미정의 다른 정보 엔트리로 유지되는 가의 여부를 조작자가 식별할 수 있도록 하는 옵션을 제공한다. 만약, 유지된다면, 작업은 데이터 엔트리를 완료하거나 및/또는 처리를 위해 저작물을 릴리즈하기 위하여 다른 활동을 대기하는 새로운 콘텐츠 요구 처리(802)의 큐에 추가된다. 일단, 저작물이 릴리즈되면, 워크 플로우 관리자(154)는 지정된 정보를 평가하여, 작업이 어떠한 처리에 전달될 것인가를 판단한다.

콘텐츠 제공자(들)(101)의 데이터베이스(160)에 자동화된 질의를 할 수 있도록 적절한 정보가 제공되면, 작업은 자동 메타 데이터 취득 처리(803)를 위해 큐된다. 데이터베이스 맵핑 표가 자동 메타 데이터 취득 처리(803)를 위해 구성되어 있지 않으면, 작업은 수동 메타 데이터 엔트리 처리(804)(데이터베이스 맵핑 표에 대한 상세한 것은 자동 메타 데이터 취득 처리(803) 섹션을 참조함)를 위해 큐된다.

오디오 처리를 위해 필요한 일반 정보 및 워터마킹을 위해 필요한 특수 정보가 지정되면, 작업은 워터마킹 처리(808)(콘텐츠 처리의 제 1 단계임)를 위해 큐된다. 작업이 제공될 때, 필요한 정보중 일부가 없다면, 작업은 부재중인 정보를 나타내는 상태와 함께 저작물 대기 활동/정보 처리의 큐로 큐된다.

상태가 콘텐츠(113)의 파일명, 예컨대 콘텐츠(113)가 오디오이고 PCM 또는 WAV 파일이 부재중임을 표시하면, 이때 입수(또는, 디지털 미디어로부터의 디지털 추출)가 필요함을 표시한다. 오디오 처리 기능에서는 곡 파일이 표준 파일 시스템을 통해 액세스될 수 있어야 한다. 만약, 곡이 오디오 처리 툴에 직접 액세스될 수 없는 파일 시스템 또는 외부 매체에 배치된다면, 파일은 우선 액세스가능한 파일 시스템으로 카피된다. 만약, 곡들이 CD나 디지털 테이프가 아닌 디지털 포맷이라면, 이들은 오디오 처리 툴에 액세스될 수 있는 파일 시스템으로 추출된다. 일단, 파일이 액세스될 수 있으면, 워크 플로우 관리자 사용자 인터페이스(700)는 워터마킹이 지정되기 위해 필요한 모든 다른 정보를 취한 워터마킹 처리에 릴리즈될 수 있도록 작업에 대한 경로 및 파일명을 지정 또는 선택하기 위해 이용된다.

3. 자동 메타 데이터 취득 처리(803)

자동 메타 데이터 취득 처리(803)는 자동화된 방식으로 가능한 많은 저작물 정보를 얻기 위하여 데이터가 수입된 콘텐츠 제공자(들)(101)의 데이터베이스 또는 스테이징 데이터베이스에 일련의 질의들을 수행한다. 자동 메타 데이터 취득 처리(803)는 아이টে를 그 큐에 배치하지 전에 다음의 정보를 필요로 한다:

- 콘텐츠 제공자(들)(101)의 데이터베이스(160)에 질의를 발생하기 위해 적절한 정보를 갖춘 데이터베이스 맵핑 표 • 질의를 수행하기 위해 필요한 저작물 정보 • 저작물을 유일하게 규정하기 위한 적절한 저작물 정보자동화된 질의가 상기 콘텐츠(113)에 필요한 정보를 얻기 위하여 콘텐츠 제공자(들)(101)의 데이터베이스(160)에 수행된다. 예를 들어, 콘텐츠(113)가 음악이면, 상기 질의를 수행하기 위해 필요한 정보는 앨범명이거나, 또는 콘텐츠 제공자(들)(101)에 의해 규정된 바와 같이 UPC 또는 특정 앨범 또는 선택 ID일 수 있다. 확보된 정보중 일부는 필요에 따라 명시될 수 있다(상세한 것은 자동 메타 데이터 취득 처리(803)에서의 선택을 참조함). 모든 필요한 정보가 확보되면, 작업은 사용 조건 처리(805)를 위해 다음에 큐된다. 소정의 필요한 정보가 부재중이면, 곡은 수동 메타 데이터 엔트리 처리(804)를 위해 큐된다. 저작물 대기 활동/정보 처리(801) 큐에서의 소정의 작업들이 상기 단계에서 확보된 정보중 일부를 대기하고 있으면, 작업 상태는 상기 정보를 더 이상 대기하고 있지 않음을 표시하기 위해 갱신된다. 만약, 작업이 더 이상 소정의 현저한 조건을 취하지 않으면, 다음의 규정된 큐로 큐된다.

4. 수동 메타 데이터 엔트리 처리(804)

수동 메타 데이터 엔트리 처리(804)는 조작자가 부재 정보를 기입할 수 있도록 하는 수단을 제공한다. 일단, 모든 필요한 정보가 지정되면, 작업은 사용 조건 처리(805)를 위해 큐된다.

5. 사용 조건 처리(805)

사용 조건 처리(805)는 저작물 이용 및 제한의 명세를 허용한다. 사용 조건 처리(805)는 소정의 메타 데이터를 필요로 한다. 사용 조건 명세의 완료시, 작업은 감시 릴리즈 처리(806) 옵션이 요구되지 않았거나 또는 워크 플로우 관리자(154) 규칙에서의 디폴트로 구성되지 않으면, 메타 데이터 SC(들) 생성 처리를 위해 큐되는 것이 적합하다. 이 경우, 작업은 감시 릴리즈 처리(806)를 위해 큐된다. 메타 데이터 SC(들) 생성 처리(807)를 큐잉하기 전에, 워크 플로우 관리자(154)는 우선 상기 처리에 대한 모든 종속 처리가 이루어졌는 가를 보증한다(이하에 참조됨). 만약, 보증되지 않으면, 작업은 저작물 대기 활동/정보 처리(801)로 큐된다.

6. 감시 릴리즈 처리(806)

감시 릴리즈 처리(806)는 디지털 콘텐츠 저작물에 지정된 정보의 품질 검사 및 유효화를 가능하게 한다. 이것은 어떠한 중속 처리도 갖지 않는다. 상기 저작물에 대한 처리의 소정의 단계에서 작업에 미리 첨부된 콘텐츠는 감시자 및 취해진 적절한 활동을 통해 재검토된다. 모든 정보 및 코멘트를 개검토한 후, 감시자는 다음의 옵션들을 취한다:

- 메타 데이터 SC(들) 생성 처리(807)를 위한 저작물의 릴리즈 승인 및 큐 · 메타 데이터 SC(들) 생성 처리(807)를 위한 저작물의 큐, 수정 및/또는 정보 부가 · 코멘트를 작업에 부가하고, 수동 메타 데이터 엔트리 처리(804)를 위해 다시 큐함 · 코멘트를 부가하고, 저작물 대기 활동/정보 처리(801) 큐로 작업을 큐시킴
- 7. 메타 데이터 SC(들) 생성 처리(807)

메타 데이터 SC(들) 생성 처리(807)는 상기 수집된 모든 정보와 더불어 메타 데이터 SC(들)(620)에 필요한 다른 정보를 함께 모아 서, 메타 데이터 SC(들)(620)를 생성하기 위해 SC(들) 패커처리를 호출한다. 상기 톨은 다음의 것들을 입력으로 필요로 한다:

- 요구된 메타 데이터 · 사용 조건 · 상기 저작물에 대한 모든 품질 레벨의 암호화 단계에서 이용되는 암호화 키상기 마지막 중속부는 메타 데이터 SC(들)(620)가 생성될 수 있기 전에 연관된 오디오 객체들이 오디오 처리 단계를 완료해야 한다. 메타 데이터 SC(들) 생성 처리(807)의 완료시, 작업은 규정된 워크 플로우 규칙들에 기초하여 최종 품질 보증 처리(813) 또는 콘텐츠 분산 처리(814)에 대한 큐로 큐된다.

8. 워터마킹 처리(808)

워터마킹 처리(808)는 저작권 및 다른 정보를 콘텐츠(113)에 부가한다. 콘텐츠(113)가 곡인 예에서, 상기 톨은 다음과 같은 것을 입력으로 필요로 한다:

- 곡 파일명(들)(앨범이면 다수의 파일명임) · 워터마킹 명령 · 워터마킹 파라미터(워터마크에 포함될 정보임)워터마킹 처리(808)의 완료시, 작업은 그 필요한 입력이 이용될 수 있으면, 전처리 및 압축 처리(809)를 위해 큐되며, 그렇지 않으면 저작물 대기 활동/정보 처리(801)로 큐된다.

9. 전처리 및 압축 처리(809)

전처리 및 압축 처리(809)는 우선 소정의 필요한 전처리를 수행하는 지정된 압축 레벨로 콘텐츠(113)를 인코딩한다. 작업을 상기 큐에 큐잉시키면 실제로 다중 큐 엔트리를 생성할 수 있다. 작업 소망하는 저작물의 각 압축 레벨로 생성된다. 인코딩 처리는 다중 시스템에서 병렬로 수행될 수 있다. 상기 톨은 다음의 입력을 필요로 한다:

- 워터마크된 콘텐츠 파일명(들)(콘텐츠(113)가 앨범이면 다중 파일명) · (미리 구성될 수 있는)저작물에 대한 품질 레벨 · (미리 구성될 수 있는)압축 알고리즘 · (전처리기에서 필요하다면)제품 장르인코딩 처리의 완료시, 작업은 워크 플로우 규칙에 따라 구성된다면, 콘텐츠 품질 제어 처리(810)를 위해 큐된다. 만약, 그렇지 않다면, 작업은 암호화 처리(811)를 위해 큐된다.

인코딩 톨의 제 3자 대상의 제공자가, 처리된 오디오 같은 콘텐츠(113)의 비율을 디스플레이하는 방법 또는 선택된 콘텐츠(113)의 전체 선택 비율로서 인코딩된 콘텐츠(113)의 양을 표시하기 위한 방법을 제공하지 않는 경우, 도 11에는, 도 8의 콘텐츠 전처리 및 압축 톨에 대한 디지털 콘텐츠의 인코딩 레이트를 판단하기 위한 방법의 흐름도(1100)가 도시된다. 이 방법은 소망하는 인코딩 알고리즘 및 비트 레이트의 선택으로 스텝(1101)을 개시한다. 다음에, 상기 알고리즘 및 인코딩 레이트가 이미 계산된 레이트 인자를 갖는가를 판단하기 위한 질의가 스텝 1102에서 이루어진다. 레이트 인자는 특정한 인코딩 알고리즘 및 특정한 비트 레이트에 대한 압축률을 판단하기 위해 이용된 인자이다. 미리 계산된 레이트 인자가 저장되어 있지 않다면, 콘텐츠(113)의 샘플은 미리 결정된 범위의 시간동안 인코딩된다. 바람직한 실시예에서 미리 결정된 시주기는 수 초이다. 미리 결정된 시 주기동안의 상기 인코딩 레이트는 새로운 레이트 인자 R

NEW를 계산하기 위해 이용된다. 스텝 1108에서, 콘텐츠(113)의 양 및 시간량을 알고 있는 새로운 레이트 인자 R

NEW의 계산은 $R_{NEW} = (\text{인코딩된 디지털 콘텐츠의 길이})/(\text{시간량})$ 이다. 스텝 1109에서, 콘텐츠(113)가 인코딩되고, 인코딩 상태는 미리 계산 레이트 인자 R

NEW를 이용하여 디스플레이된다. 이후, 스텝 1107에서, 상기 인코딩 레이트 인자 R

NEW가 상기 인코딩 알고리즘 및 인코딩 비트 레이트에 대한 앞으로의 이용을 위해 저장된다. 스텝 1103에서, 선택된 알고리즘이 미리 계산된 레이트 인자 R

STORED를 갖는다면, 스텝 1104에서, 콘텐츠(113)는 인코딩되고, 이어서 미리 계산된 레이트 인자 R_{STORED} 를 이용하여 디스플레이된다. 한편, 스텝 1105에서, 상기 현재의 레이트 인자 R

CURRENT가 상기 선택된 알고리즘 및 비트 레이트에 대하여 계산된다. 스텝 1106에서, 상기 현재 레이트 인자 R

CURRENT는 기억된 레이트 인자 R_{NEW} 가 $(R_{STORED} + R_{CURRENT})$ 의 평균과 같도록 갱신하기 위해 이용된다. 레이트 인자의 반복적인 갱신으로 인코딩 레이트의 판단이 특정한 인코딩 알고리즘 및 비트 레이트에 대한 각 다음의 이용시 더욱 정확하게 되도록 할 수 있

다. 이후, 새로운 레이트 R

NEW가 스텝 1107에서 앞으로의 이용을 위해 저장된다. 현재의 레이트 인자 R

CURRENT가 주어진 범위 또는 임계치로 미리 저장된 레이트 인자 R_{STORED} 의 범위를 넘는다면 R_{STORED} 의 갱신이 이루어질 수 없다.

이어서, 인코딩 상태의 디스플레이가 나타날 수 있다. 인코딩 상태는 콘텐츠(113)에 대한 파일의 전체 길이 및 인코딩 레이트에 기초하여 진행 막대로서 디스플레이된 전체 콘텐츠(113) 비율의 디스플레이와 함께 현재 인코딩 레이트를 포함한다. 인코딩 상태는 또한 인코딩을 위해 남은 시간을 포함할 수 있다. 인코딩을 위해 남은 시간은 R

CURRENT로 계산된 인코딩 레이트를 콘텐츠(113)에 대한 파일의 전체 길이로 나눔으로써 계산될 수 있다. 인코딩 상태는 호출 처리를 불러올 수 있는 다른 프로그램에 전달될 수 있다. 이것은 더 효율적인 처리를 위해 조작 및 일괄 처리되는 인코딩시 인코딩에 대한 감시 프로그램 또는 공동-종속 프로그램을 지원한다. 다른 실시예에서, 인코딩은 워터마킹 단계를 포함할 수 있음이 이해되어야 한다.

10. 콘텐츠 품질 제어 처리(810)

콘텐츠 품질 제어 처리(810)는 감시 릴리즈 처리(806)와 기능적으로 유사하다. 이에 따라 누군가가 멀리서 수행된 콘텐츠 처리의 품질을 확인할 수 있도록 하는 선택적 단계가 있다. 이것은 전처리 및 압축 처리(809)의 인코딩 부분 및 워터마킹 처리(808)의 완료와는 달리 어떠한 종속성도 없다. 콘텐츠 품질 제어 처리(810)의 완료시, 다음의 옵션이 이용될 수 있다:

- 작업이 암호화 처리(811)를 위해 릴리즈 및 큐될 수 있음.
- 코멘트가 첨부될 수 있으며, 하나 이상의 작업들이 전처리 및 압축 처리(809)를 위해 다시 큐됨.

최종 옵션은 곡 파일의 비인코딩된 워터마크 버전이 콘텐츠 품질 제어 처리(810) 후 까지 이용될 수 있도록 남아 있어야 한다.

11. 암호화 처리(811)

암호화 처리(811)는 적절한 워터마크된/인코딩된 곡 파일들 각각을 암호화하기 위해 보안 디지털 콘텐츠 전자 배포 권리 관리 기능을 호출한다. 상기 처리는 모든 다른 오디오 처리의 완료와는 달리 종속성이 없다. 암호화 처리(811)의 완료시, 작업은 콘텐츠 SC(들) 생성 처리(812)를 위해 큐된다.

12. 콘텐츠 SC(들) 생성 처리(812)

콘텐츠 SC(들) 생성 처리(812) 처리는 콘텐츠 SC(들)(630)에 포함될 일부 메타 데이터 파일을 필요로 한다. 콘텐츠(113)와는 다른 파일들이 요구되면, 파일들이 모이고, SC(들) 패커 처리는 생성된 콘텐츠(113)(예컨대, 곡)의 각 압축 레벨로 콘텐츠 SC(들)(630)를 생성하기 위해 호출된다. 콘텐츠 SC(들) 생성 처리(812)의 완료시, 곡은 규정된 워크 플로우 규칙에 기초하여, 최종 품질 보증 처리(813) 또는 콘텐츠 분산 처리(814) 큐로 큐된다.

13. 최종 품질 보증 처리(813)

최종 품질 보증 처리(813)는 연관된 메타 데이터 및 콘텐츠 SC(들)(630) 사이에서의 교차 참조 검색을 가능하게 하여, 이들이 정확하게 일치하고 모든 정보와 여기에 포함된 콘텐츠(113)가 정확함을 검증할 수 있도록 하는 선택적 단계이다. 최종 품질 보증 처리(813)의 완료시, 작업은 콘텐츠 분산 처리(814)를 위해 큐된다. 만약, 문제점이 발견되면, 대부분의 경우에 작업은 실패 단계로 다시 큐되어야만 한다. 이 단계에서의 재작업은 저작물이 문제를 해결하기 위해 필요한 처리와 더불어 재암호화 및 재패킹을 마쳐야만 하기 때문에, 훨씬 고가이다. 정보의 정확성 및 완전성과 콘텐츠(113)의 품질을 보증하기 위해 이용되는 이전의 보증 단계가 많이 권장된다.

14. 콘텐츠 분산 처리(814)

콘텐츠 분산 처리(814) 처리는 SC(들)을 적절한 호스팅 사이트로 전송하는 역할을 한다. SC(들)의 성공적인 전송 후에, 작업 완료 상태가 로그되고, 작업은 큐로부터 삭제된다. 만약, SC(들) 전송시 문제가 발생하면, 규정된 횟수의 재시도 후, 작업은 발생한 에러와 함께 실패됨에 따라 워크 플로우 관리자 툴(154)에 플래그된다.

15. 워크 플로우 규칙

도 8에서의 워크 플로우 규칙은 다음과 같이 3개의 주요 시스템으로 동작한다:A: 워크 플로우 관리자 툴(154)1. 새로운 콘텐츠 요구 처리(802)

2. 저작물 대기 활동/정보 처리(801)

3. 최종 품질 보증 처리(813)

4. 콘텐츠 분산(및, 통지) 처리(814)

B: 메타 데이터 융합 및 엔트리 툴(161)1. 자동 메타 데이터 취득 처리(803)

2. 수동 메타 데이터 엔트리 처리(804)

3. 감시 릴리즈 처리(806)

4. 메타 데이터 SC(들) 생성 처리(807)

C. 콘텐츠 처리 툴(155)

1. 워터마킹 처리(808)(저작권 데이터를 필요로 함)

2. 전처리 및 압축 처리(809)

3. 콘텐츠 품질 제어 처리(810)

4. 암호화 처리(811)

5. 콘텐츠 SC(들) 생성 처리(812)

워크 플로우콘텐츠(113) 선택 조작자는 새로운 저작물을 입력하고, 이것을 A1(새로운 콘텐츠 요구 처리(802))상에 큐시킨다.

A1: 콘텐츠(113) 선택 조작자가 이것을 워크 플로우 관리자 툴(154)에 릴리즈하는 경우, B1(자동 메타 데이터 취득 처리(803))으로 큐시킨다.

A2: 스텝 Before(메타 데이터 SC(들) 생성 처리(807))로 진행되는 중에, 스텝 B1(자동 메타 데이터 취득 처리(803)), 또는 스텝 B2(수동 메타 데이터 엔트리 처리(804)), 또는 스텝 B3(감시 릴리즈 처리(806))로부터 도래함[암호화 키를 필요로 함].

스텝 A3(최종 품질 보증 처리(813)) 또는 스텝 A4(콘텐츠 분산 처리(814))로 진행되는 중에, Before(메타 데이터 SC(들) 생성 처리(817))로부터 도래함[콘텐츠 SC(들)(630)을 필요로 함].

스텝 C2(전처리 및 압축 처리(809))로 진행되는 중에, 스텝 C1(워터마킹 처리(808))으로부터 도래함[전처리 및 압축 처리(809)를 위한 메타 데이터를 필요로 함].

스텝 C5(콘텐츠 SC(들) 생성 처리(812))로 진행되는 중에, 스텝 C4(암호화 처리(811))로부터 도래함[콘텐츠 SC(들)(630) 패킹을 위한 메타 데이터를 필요로 함].

스텝 A3(최종 품질 보증 처리(813)) 또는 스텝 A4(콘텐츠 분산 처리(184))로 진행되는 중에, 스텝 C5로부터 도래함[메타 데이터 SC(들)(620)을 필요로 함].

A3: 스텝 A3(최종 품질 보증 처리(813)) 후에, 큐 B2(수동 메타 데이터 엔트리 처리(804))에 배치, 또는 큐 B3(감시 릴리즈 처리(806))에 배치, 또는 품질 보증 조작자에 의해 필요에 따라 큐에 배치함.

A4: 스텝 A4(콘텐츠 분산 처리(814)) 후에, 워크 플로우 관리자 툴(154)이 상기 저작물에 대하여 작업됨.

B1: 스텝 B1(자동 메타 데이터 취득 처리(803)) 후에, 만약, 스텝 C1(워터마킹 처리(808))에 필요한 메타 데이터가 존재하면, 상기 저작물을 나타내는 엔트리를 큐 C1에 배치함(또한, 다음의 로직을 수행함).

만약, 1-소정의 필요한 메타 데이터가 없거나, 또는 2-수동 메타 데이터 제공자에게 제공된 코멘트가 있다면, 또한 저작물을 큐 B2(수동 메타 데이터 엔트리 처리(804))에 배치하고, 그렇지 않고, 감시 릴리즈가 상기 저작물에 대하여 요구된다면, 저작물을 큐 B3(감시 릴리즈 처리(806))에 배치함.

그렇지 않고, 저작물이 모든 요구된 품질 레벨에 대한 콘텐츠 처리 툴(155)로부터의 모든 정보를 갖으면, 저작물을 큐 Before(메타 데이터 SC(들) 생성 처리(807))에 배치하며, 그렇지 않으면, 저작물이 암호화 키를 필요로 하는 것으로 플래그하고, 저작물을 큐 A2(저작물 대기 활동/정보 처리(801))에 배치함.

B2: 스텝 B2(수동 메타 데이터 엔트리 처리(804))중에, 만약, 스텝 C1(워터마킹 처리(808))이 처리되지 않고, 스텝 C1에 필요한 메타 데이터가 존재하면, 상기 저작물을 나타내는 엔트리를 큐 C1에 배치함(또한, 다음의 로직을 수행함).

만약, 스텝 C2(전처리 및 압축 처리(809))에 필요한 메타 데이터가 제공되면, (또한, 다음의 로직을 수행함)만약, 메타 데이터 융합 및 엔트리 툴(161)에 의해 수집된 모든 메타 데이터가 존재하면, 이때, 만약, 감시 감시 릴리즈가 상기 저작물에 요구되었다면, 저작물을 큐 B3(감시 릴리즈 처리(806))에 배치하고, 그렇지 않고, 만약, 콘텐츠 처리 툴(155)의 스텝 C4(암호화 처리(811))으로부터의

모든 정보가 존재하면, 상기 저작물을 큐 Before(메타 데이터 SC(들) 생성 처리(807))에 배치하고, 그렇지 않으면, 저작물을 암호화 키를 필요로 하는 것으로 플래그하고, 이 저작물을 큐 A2(저작물 대기 활동/정보(801))에 배치함.

그렇지 않고, 만약, 메타 데이터 제공자가 강제적 감시 릴리즈를 요구하면, 저작물을 큐 B3(감시 릴리즈 처리(806))에 배치하고, 그렇지 않으면, 이외에 아무것도 수행하지 않는다(예컨대, 큐 B2(수동 메타 데이터 엔트리 처리(804))에 저작물을 유지시키지 않음).

B3: 스텝 B3(감시 릴리즈 처리(806))중에, 만약, 상기 조작자가 저작물을 스텝 B2(수동 메타 데이터 엔트리 처리(804))로 다시 전송하면, 저작물을 큐 B2에 배치함.

그렇지 않고, 상기 조작자가 저작물을 릴리즈하면, 이때, 만약, 콘텐츠 처리 툴(155)의 스텝 C4(암호화 처리(811))로부터의 모든 정보가 존재하는 경우, 상기 저작물을 큐 Before(메타 데이터 SC(들) 생성 처리)에 배치하고, 그렇지 않으면, 저작물을 암호화 키가 필요한 것으로 플래그하고, 이 저작물을 큐 A2(저작물 대기 활동/정보 처리(801))에 배치함.

그렇지 않으면, 저작물은 큐 B3(감시 릴리즈 처리(806))에 남는다.

Before: 스텝 Before(메타 데이터 SC(들) 생성 처리(807)) 후에, 메타 데이터가 팩된 저작물을 플래그함.

만약, 모든 (저작물/품질 레벨) 튜플(tuple)이 팩되었다면, 이때, 만약, 콘텐츠 제공자(들)(101) 구성이 품질 보증 SC(들)를 지정하면, 이 저작물을 큐 A3(최종 품질 보증 처리(813))에 배치하고, 그렇지 않으면, 이 저작물을 큐 A4(콘텐츠 분산 처리(814))에 배치함.

그렇지 않으면, 저작물이 콘텐츠(113) SC(들)가 필요한 것으로 플래그하고, 이 저작물을 큐 A2(저작물 대기 활동/정보 처리(801))에 배치함. C1: 스텝 C1(워터마킹 처리(808)) 후에, 만약, 스텝 C2(전처리 및 압축 처리(809))에 필요한 메타 데이터가 존재하면, 각 (저작물/품질 레벨) 튜플에 대한 엔트리를 생성하고, 이들을 큐 C2에 배치하고, 그렇지 않으면, 저작물이 전처리/압축을 위한 메타 데이터를 필요로 하는 것으로 플래그하고, 이 저작물을 큐 A2(저작물 대기 활동/정보 처리(801))에 배치함.

C2: 스텝 C2(전처리 및 압축 처리(809)) 이후, 만약, 콘텐츠 제공자(101)의 구성이 콘텐츠 품질 제어 처리(810)를 지시하면, 이 (저작물/품질 레벨) 튜플을 큐 C3(콘텐츠 품질 제어 처리(810))에 배치하고, 그렇지 않으면, 이 (저작물/품질 레벨) 튜플을 큐 C4(암호화 처리(811))에 배치함.

C3: 스텝 C3(콘텐츠 품질 제어 처리(810)) 이후, 이 (저작물/품질 레벨) 튜플을 큐 C4(암호화 처리(811))에 배치함.

C4: 스텝 C4(암호화 처리(811)) 이후, 메타 데이터 융합 및 엔트리 툴(161)에 필요한 정보를 제공하고, 만약, 콘텐츠 SC(들)(630)에 필요한 모든 메타 데이터가 존재하면, 이 (저작물/품질 레벨) 튜플을 큐 C5(콘텐츠 SC(들) 생성 처리(812))에 배치하고, 그렇지 않으면, 저작물을 콘텐츠 SC(들)(630)에 대한 메타 데이터를 필요로 하는 것으로 플래그하고, 이 (저작물/품질 레벨) 튜플을 A2(저작물 대기 활동/정보 처리(801))에 배치함.

C5: 스텝 C5(콘텐츠 SC(들) 생성 처리(812)) 후에, 이미 팩된 상기 품질 레벨로 품질 레벨 콘텐츠(113)를 플래그함.

만약, 모든 (저작물/품질 레벨) 튜플이 팩되었다면, 이때, 만약, 저작물이 메타 데이터가 팩된 것으로 플래그되면, 이때, 만약, 콘텐츠 제공자(들)(101)의 구성이 품질 보증 SC(들)를 지정하면, 이 저작물을 큐 A3(최종 품질 보증 처리(813))에 배치함.

그렇지 않으면, 이 저작물을 큐 A4(콘텐츠 분산 처리(814))에 배치함.

그렇지 않으면, 저작물을 메타 데이터 SC(들)(620)가 필요한 것으로 플래그하고, 이 저작물을 큐 A2(저작물 대기 활동/정보 처리(801))를 대기하는 저작물) 배치함.

그렇지 않으면, (모든 (저작물/품질 레벨) 튜플이 팩되지 않아서) 아무것도 수행하지 않음(예컨대, 다른 (저작물/품질 레벨) 튜플이 활동을 트리거함).

C. 메타 데이터 융합 및 엔트리 툴

메타 데이터는 예컨대, 음악에서 녹음의 타이틀, 가수, 작사/작곡가, 프로듀서 및 녹음의 길이 같은 콘텐츠(113)를 설명하는 데이터로 구성된다. 다음의 설명이 음악인 콘텐츠(113)에 기초되지만, 예컨대, 비디오, 멀티미디어, 영화 등의 다른 콘텐츠 타입이 본 발명의 범주 및 사상에 있을 수 있음을 당 기술에 숙련된 지식을 가진 자들은 이해할 것이다.

상기 보조 시스템은, 콘텐츠 제공자(들)(101)가 저작물의 판매를 촉진하는데 도움을 주기 위하여 전자 디지털 콘텐츠 스토어(들)(103)에 제공하는 데이터(예컨대, 음악에서, 상기 가수에 의한 샘플 클립, 상기 가수의 경력, 상기 녹음이 출판된 앨범의 목록, 상기 가수 및/또는 저작물과 연관된 장르), 콘텐츠 제공자(들)(101)가 최종 사용자(들)에게 구매된 저작물을 제공한 데이터(예컨대, 가수, 프로듀서, 앨범 표지, 트랙 길이), 및 콘텐츠 제공자(들)(101)가 최종 사용자(들)에게 제공하고자 하는 다른 구매 옵션(사용 조건(517))을 함께 취한다. 데이터는 메타 데이터 SC(들)(620)로 패키징되며, 전자 디지털 콘텐츠 스토어(들)(103)에 이용될 수 있다. 이를 구현하기 위하여, 다음의 툴들이 제공된다:

· 자동 메타 데이터 취득 툴 · 수동 메타 데이터 엔트리 툴 · 사용 조건 툴 · 감시 릴리즈 툴
상기 툴들은 워크 플로우 관리자(154)에 상술된 처리를 실행할 수 있도록 한다. 여기서 설명된 툴들은 양호한 실시예에서의 자바에 기초한 툴킷이지만, C/C++, 어셈블러 등의

다른 프로그래밍 언어가 이용될 수도 있다.

1. 자동 메타 데이터 취득 툴

자동 메타 데이터 취득 툴은 상술된 자동 메타 데이터 취득 처리(803)를 실행하기 위한 기능을 사용자에게 제공한다. 자동 메타 데이터 취득 툴은 콘텐츠 제공자(들)(101)의 데이터베이스(160)에 액세스하기 위해서, 및 조작자 도움없이 가능한 많은 데이터를 검색하기 위해서 이용된다. 구성 방법은 상기 처리를 자동화하기 위하여 이용될 수 있다. 콘텐츠 제공자(들)(101)는, 상기 콘텐츠 제공자(들)(101)가 최종 사용자(들)에게 제공하고자 하는 데이터(예컨대, 작곡자, 프로듀서, 연주자, 트랙 길이)의 타입과, 콘텐츠 제공자(들)(101)가 전자 디지털 콘텐츠 스토어(들)(103)에게 제공하는 프로모션형 데이터(예컨대, 음악에서, 상기 가수에 의한 샘플 클립, 상기 가수의 경력, 상기 녹음이 출판된 앨범의 목록 및 상기 가수와 연관된 장르)의 타입을 식별하기 위하여 디폴트 메타 데이터 템플릿을 요건에 맞도록 할 수 있다. 디폴트 메타 데이터 템플릿은 최종 사용자 장치(들)(109)에 필요한 데이터 필드, 최종 사용자 장치(들)(109)에 선택적으로 제공될 수 있는 데이터 필드, 및 가수, 앨범 및/또는 싱글을 프로모션하는 전자 디지털 콘텐츠 스토어(들)(103)에 타겟된 데이터 필드의 샘플 세트를 포함한다.

콘텐츠 제공자(들)(101)의 데이터베이스(160)로부터 템플릿 데이터 필드를 추출하기 위하여, 자동 메타 데이터 취득 툴은 데이터가 발견될 수 있는 데이터베이스 내의 장소에 데이터(예컨대, 작곡자, 프로듀서, 가수의 일대기)의 타입을 맵시킨 표를 이용한다. 각 콘텐츠 제공자(들)(101)는 그들의 환경에 대한 맵핑표를 작성하는데 도움을 준다.

자동 메타 데이터 취득 툴은 데이터가 콘텐츠 제공자(들)(101)의 데이터베이스(160)로부터 이용가능할 때마다 이 데이터를 취득하기 위하여 맵핑표와 콘텐츠 제공자(들)(101)의 메타 데이터 템플릿을 이용한다. 각 저작물의 상태는 자동 메타 데이터 취득 처리(803)의 결과로 갱신된다. 소정의 필요한 데이터가 부재중인 저작물은 수동 메타 데이터 엔트리 처리(804)를 위해 큐되며, 그렇지 않다면 메타 데이터 SC(들)(620)로 패키징하기 위하여 이용될 수 있다.

2. 수동 메타 데이터 엔트리 툴

수동 메타 데이터 엔트리 툴은 상술된 수동 메타 데이터 엔트리 처리(804)를 실행하기 위한 기능을 사용자에게 제공한다. 수동 메타 데이터 엔트리 툴은 소정의 정당하게 인증된 조작자가 부재중인 데이터를 제공할 수 있도록 한다. 조작자는 부재중인 데이터가 이용될 수 없다고 판단하면, 조작자는 저작물에 코멘트를 붙이고, 감시 릴리즈를 요구한다. 콘텐츠 제공자(들)(101)는 저작물이 감시 릴리즈를 받고 있는 품질 보증 이유를 요구할 수 있다. 일단, 모든 필요한 데이터가 존재하고, 감시 릴리즈가 요구되지 않았다면, 이때 저작물은 메타 데이터 SC(들)(620)로 패키징하기 위해 이용될 수 있다.

3. 사용 조건 툴

사용 조건 툴은 상술된 사용 조건 처리(805)를 실행하기 위한 기능을 사용자에게 제공한다. 전자 배달을 이용하여 판매 또는 렌트(제한적으로 이용됨)하기 위한 오퍼링 콘텐츠(113)의 처리는 일련의 사업 결정을 수반한다. 콘텐츠 제공자(들)(100)는 이용될 수 있는 압축 레벨(들)의 콘텐츠(113)인 가를 결정한다. 콘텐츠(113)의 각 압축되어 인코딩된 버전마다 하나 이상의 사용 조건들이 지정된다. 각 사용 조건은 콘텐츠(113)의 사용과 관련하여 최종 사용자(들)에서의 소정의 제한 및 최종 사용자(들)의 권리를 규정한다.

콘텐츠 처리 툴(155) 부분에서, 사용 조건(최종 사용자(들) 권리 및 제한)의 세트가 저작물에 첨부된다.

사용 조건을 정의함: 1. 상기 사용 조건이 적용되는 콘텐츠(113)의 압축 인코딩된 버전.

2. 상기 사용 조건(예컨대, 사업, 개인 고객)이 미치는 사용자의 타입.

3. 상기 사용 조건이 콘텐츠(113)의 구매 또는 렌탈을 허용하는가의 여부.

렌탈 트랜잭션에 대하여: • 렌탈 기간(예컨대, 날짜, 플레이)을 제한하기 위해 이용된 측정 유닛.

• 콘텐츠(113)가 더 이상 플레이될 수 없는 상기 유닛의 수.

구매 트랜잭션에 대하여: • 최종 사용자(들)에게 허용된 플레이가능한 카피의 수 • 상기 카피가 이루어질 수 있는 매체(예컨대, CD-기록가능한(CD-R), 미니디스크, 퍼스널 컴퓨터)의 종류.

4. 구매/렌탈 트랜잭션 발생이 허용될 수 있는 기간의 주기(즉, 최종 사용자(들)는 최초 이용일 이후에서 최종 이용일 전에만 상기 사용 조건의 기간하에서 구매/렌탈할 수 있음).

5. 최종 사용자(들)가 상기 구매(또는, 렌탈)를 트랜잭션할 수 있는 국가.

6. 상기 사용 조건하에서의 구매/렌탈 트랜잭션의 가격.

7. 워터마킹 파라미터.

8. 클리어링하우스(들)(105)의 통지를 필요로 하는 사건의 타입.

사용 조건 세트의 예컨대 콘텐츠 제공자(들)(101)는 1997년 4사분기중에 대중적인 어린이의 보컬리스트에 의해 어린이를 위한 곡의 재발매에 관한 북미 시장 승인을 시험하기 위한 결정을 할 수 있다. 이 시험은 2개의 다른 압축 인코딩 버전들: 384Kbps 및 56Kbps로 이용될 수 있는 곡을 만들 수 있다. 384Kbps 버전은 구입(및, 하나의 카피가 미니 디스크상에서 이루어질 수 있음) 또는 렌트(2주 기간 동안)될 수 있으며, 반면 56Kbps 버전은 구입만될 수 있다(그리고, 카피는 될 수 없다). 워터마킹 명령은 어떠한 구매/렌탈에 대해서도 동일하며, 콘텐츠 제공자(들)(101)는 클리어링하우스(들)(105)가 이루어질 수 있는 매 카피를 카운트할 수 있기를 원한다. 이것은 다음과 같은 사용 조건을 생성한다:

	사용조건 1	사용조건 2	사용조건 3
압축 인코딩된 버전	384 Kbps	384 Kbs	56 Kbps
유저의 타입	개인 고객	개인 고객	개인 고객
트랜잭션의 타입	구매	렌탈	구매
이용가능 일자	1 Oct 1997 - 31 Dec 1997	1 Oct 1997 - 31 Dec 1997	1 Oct 1997 - 31 Dec 1997
국가	미국 및 캐나다	미국 및 캐나다	미국 및 캐나다
워터마킹	std.	std.	std.
사건통지	카피 활동	없음	없음
카피의 횟수	1	0	0
어떤 매체로	미니 디스크	적용 불가	적용 불가
렌탈 기간	적용불가	14 일	적용 불가
가격	가격 1	가격 2	가격 3

4. 메타 데이터 SC(들)(620)의 부분

하기에는 메타 데이터 용합 및 엔트리 툴(161)이 메타 데이터 SC(들)(620)로 수반을 위해 수집한 일부 데이터의 유형이 있다. 데이터를 기능 및 목적에 따라 SC(들)로 그룹화하기 위한 시도가 이루어지게 된다.

저작물 ID [src:content provider;] [dest:everybody;]인가 레이블 회로 [dest:EMS;end-user;]인가 레이블 회로 [dest:EMS;end-user;]상기 객체(보조 인가 레이블 회사)의 소스(발행자) [dest:everybody]객체의 타입(즉, 단일 객체 또는 객체의 어레이)

객체 ID [dest:everybody;]

국제 표준 기록 코드(ISRC)국제 표준 음악 번호(ISMN)사용조건(src:콘텐츠제공자;dest:EMS,최종 사용자,클리어링하우스(들)(105))구입된 사용 조건 (src:EMS;dest:최종 사용자,클리어링하우스(들)(105))객체(사운드 녹음)의 이용을 위한 사용 조건의 세트(고객 제한 및 권리)상기 사용 조건이 적용되는 콘텐츠(113)의 압축 인코딩된 버전상기 사용 조건이 콘텐츠(113)의 구매 또는 렌탈을 허용하는가의 여부렌탈 트랜잭션에 대하여:렌탈 기간(예컨대, 날짜, 플레이)을 제한하기 위해 이용된 측정 유닛.

콘텐츠(113)가 더 이상 플레이될 수 없는 상기 유닛의 수.

구매 트랜잭션에 대하여:최종 사용자(들)에게 허용된 플레이가능한 카피의 수상기 카피가 이루어질 수 있는 매체(예컨대, CD-기록가능한(CD-R), 미니디스크, 퍼스널 컴퓨터)의 종류.

구매/렌탈 트랜잭션 발생이 허용될 수 있는 기간의 주기(즉, 최종 사용자(들)는 최초 이용일 이후에서 최종 이용일 전에만 상기 사용 조건의 기간하에서 구매/렌탈할 수 있음)최종 사용자(들)가 상기 구매(또는, 렌탈)를 트랜잭션할 수 있는 국가의 포인터상기 사용 조건하에서의 구매/렌탈 트랜잭션의 가격암호화된 워터마킹 명령 및 파라미터의 포인터클리어링하우스(들)(105)의 통지를 필요로 하는 사건의 타입 포인터구매 데이터(암호화된; 선택적 정보; src: EMS; dest: 최종 사용자, 클리어링하우스(들)(105))구매 일자구매 가격이름 및 주소에 대한 빌고객 이름 및 주소고객의 국가(최상의 게스트)메타 데이터 1 (src: 콘텐츠 제공자; dest: EMS, 최종 사용자)~의 어레이(an array of){저작권 정보정보에 대한(for the composition)사운드 녹음에 대한(for the sound recording)곡의 타이틀주요 가수(들)}~에 대한 포인터(a pointer to){삽화(예컨대, 앨범 표지);삽화의 포맷(예컨대, GIF, JPEG);}선택적 정보:부가 정보의 어레이{작곡자발행자프로듀서연주자녹음일발매일(date of release)가사트랙명(설명)/트랙 길이상기 녹음이 나타나는 앨범의 리스트장르(들)}메타 데이터 2 (src: 콘텐츠 제공자; dest:EMS)구성들의 어레이, 각각은 동일한 사운드 녹음의 다른 품질 레벨을 나타냄{사운드 녹음;사운드 녹음의 품질 레벨;(아마도 압축된)사운드 녹음의 (바이트로)크기;}메타 데이터 3 (src: 콘텐츠 제공자; dest: EMS, 최종 사용자)선택적 정보:프로모션형 자료:가수 프로모션 자료에 대한 포인터{가수의 웹 사이트로 URL;가수(들)의 배경 설명(들);가수-관련 인터뷰(인터뷰의 포맷(예컨대, 텍스트, 오디오, 비디오)도 함께함);평론(평론의 포맷(예컨대, 텍스트, 오디오, 비디오)도 함께함);샘플 클립(및, 그 포맷과 압축 레벨);최근 및 곧이어 있을 콘서트/출판/이벤트-이들의 일자 및 장소;}앨범 프로모션 자료에 대한 포인터{샘플 클립(및, 그 포맷 및 압축 레벨);프로듀서, 및/또는 작곡자, 및/또는 영화/상연/캐스트, 및/또는 앨범위 제작 등의 배경 설명(들);비-가수-관련 인터뷰(인터뷰의 포맷(예컨대, 텍스트, 오디오, 비디오)와 함께함);평판(평판의 포맷(예컨대, 텍스트, 오디오, 비디오)과 함께함);장르(들);}단일 프로모션:샘플 클립(및, 그 포맷 및 압축 레벨)프로듀서, 및/또는 작곡자, 및/또는 영화/상연/캐스트, 및/또는 앨범위 제작 등의 배경 설명(들);평판(평판의 포맷(예컨대, 텍스트, 오디오, 비디오)과 함께함);5. 감시 릴리즈 툴

감시 릴리즈 툴은 상술된 감시 릴리즈 처리(806)를 실행하기 위한 기능을 사용자에게 제공한다. 감시 릴리즈 권한을 갖는 것으로 콘텐츠 제공자(들)(101)에 의해 지시된 개체는 저작물 대기 감시 릴리즈(즉, 감시 릴리즈 처리(806)의 큐상에서의 저작물)를 호출하고,

그 콘텐츠(113) 및 수반된 코멘트를 검사하고,

그 콘텐츠(113)를 승인하고, 메타 데이터 SC(들)(620)로 패키징하기 위해 저작물을 릴리즈하거나, 또는,

소정의 필요한 수정을 가하고, 메타 데이터 SC(들)(620)를 패키징하기 위해 저작물을 릴리즈하거나, 또는, 취해야 할 수정 활동을 지정하기 위한 코멘트를 추가하고, 저작물을 수동 메타 데이터 엔트리 처리(704)로 재전달한다.

다른 실시예에서, SC(들)의 생성 후, 다른 선택적 품질 보증 단계가 있는데, 여기서 SC(들)의 콘텐츠(113)가 열려서 완전성 및 정확성을 검사받을 수 있으며, 이때, 최종 승인은 소매 채널로의 저작물의 릴리즈를 위하여 주어지거나 또는 거부될 수 있다.

D. 콘텐츠 처리 툴

콘텐츠 처리 툴(155)은 실질적으로 콘텐츠의 카피에 워터마크, 인코드 및 암호화를 생성하도록 디지털 콘텐츠 파일을 처리하기 위해 이용되는 소프트웨어 툴의 집합이다. 이 툴은 이들이 수반하는 워터마킹, 인코딩 및 암호화 기술의 플러그 가능한 대체를 허용하기 위해 산업 표준 디지털 콘텐츠 처리 툴을 이용한다. 만약, 선택된 산업 툴이 명령 라인 시스템 호출 인터페이스 및 전달된 파라미터를 통해 로드되거나, 기능이 DLL 인터페이스를 통해 호출될 수 있는 툴킷을 제공할 수 있다면, 콘텐츠 처리는 어느 정도 자동화될 수 있다. 각 툴로의 프론트 엔드 애플리케이션은 다음에 이용가능한 작업을 위해 콘텐츠 처리 툴(155)에서의 적절한 큐에 질의하고, 요구된 파일 및 파라미터를 검색한 후, 요구된 기능을 수행하기 위하여 산업 표준 콘텐츠 처리 툴을 로드한다. 태스크의 완료시, 툴이 종료 상태를 보고하지 않는다면, 큐 대한 수동 갱신이 필요하게 된다.

콘텐츠 처리 툴(155)의 포괄적 버전이 설명되었지만, 개별화도 가능하다. 콘텐츠 처리 툴(155)은 자바, C/C++ 또는 소정의 상응하는 소프트웨어로 기입될 수 있다. 콘텐츠 처리 툴(155)은 디스켓, CDS를 포함한 소정의 컴퓨터 판독가능 수단에 의해 웹 사이트를 통해 전달될 수 있다.

1. 워터마킹 툴

워터마킹 툴은 상술된 바와 같이 워터마킹 처리(808)를 실행하기 위한 기능을 사용자에게 제공한다. 상기 툴은 콘텐츠(113) 소유자의 저작권 정보를 오디오 워터마킹 기술을 이용하여 곡 파일에 제공한다. 기입될 실제 정보는 콘텐츠 제공자(들)(101) 및 선택된 특정한 워터마킹 기술에 의해 결정된다. 이 정보는 상기 정보를 워터마킹 기능에 적절하게 전달할 수 있도록 프론트 엔드 워터마킹 툴에 이용될 수 있다. 이것은 예를 들어 곡의 오디오 파일이 처리되도록 하기 전에 상기 정보를 취하였음을 보장하기 위하여 메타 데이터 융합 및 엔트리 툴(161)상에 동기화 요건을 부과한다. 이 곡은 워터마킹 정보가 얻어질 때까지 오디오 처리에 이용될 수 없다.

워터마크는 생성된 곡의 모든 인코딩에 공통적이기 때문에 오디오 처리에서의 제 1 단계로서 적용된다. 워터마크가 인코딩 기술을 채택하는한, 워터마킹 처리는 곡마다 한번씩만 발생될 필요가 있다.

여러 가지 워터마킹 기술이 공지되어 상용되고 있다. 프론트 엔드 워터마킹 툴이 다양한 산업 워터마킹 툴을 지원할 수 있다.

2. 전처리 및 압축 툴

전처리 및 압축 툴은 상술된 바와 같이 전처리 및 압축 처리(809)를 실행하기 위한 기능을 사용자에게 제공한다. 오디오 인코딩은 2개의 처리를 수반한다. 인코딩은 기본적으로 예컨대 PCM 오디오 스트림 같은 음악 콘텐츠에서 손실이 있는 압축 알고리즘 대항 애플리케이션이다. 인코더는 일반적으로 필요한 오디오 품질 레벨에 기초하여 여러 가지 플레이백 비트 스트림 레이트를 생성하기 위해 조정될 수 있다. 고품질은 더 큰 파일 크기를 요하며, 파일 크기가 고품질 콘텐츠(113)에서는 매우 크기 때문에, 고품질 콘텐츠(113)의 다운로드 시간은 길게 되며, 종종 표준 28,800bps 모뎀에서는 금지된다.

따라서, 콘텐츠 제공자(들)(101)는 다운로드를 위한 시간을 기다리기 원하지 않는 저대역폭 고객이나, 또는 고품질 콘텐츠(113)만을 구입하고자 하거나 고속 접속을 갖는 오디오 애호가나 고대역폭 고객 모두의 불편함을 완화시키기 위하여 다운로드에 다양한 디지털 콘텐츠 품질을 공급하기 위한 선택을 할 수 있다.

압축 알고리즘은 콘텐츠(113)의 저비트율 재생을 이루기 위해 그 기술이 변화된다. 기술은 알고리즘(즉, MPEG, AC3, ATRAC) 및 압축 레벨 모두에 의해 변화된다. 더 높은 압축 레벨을 얻기 위해, 일반적으로 데이터는 압축 알고리즘에 전달되기 전에 저 샘플링 레이트로 재샘플링된다. 적은 충실도의 손실로 더 효율적인 압축을 제공하기 위해, 또는 일부 주파수 범위의 극단적인 드롭아웃을 방지하기 위하여, 디지털 콘텐츠는 종종 소정의 주파수 등화 레벨로의 조정 또는 녹음의 강약 변화의 조정을 필요로 할 수 있다. 콘텐츠 전처리 요건은 필요한 압축 레벨 및 압축 알고리즘에 직접 관련된다. 일부 경우에, 콘텐츠(113)의 스타일(예컨대, 음악적 장르)은, 일부 장르에서의 곡이 유사한 강약 변화를 갖을 수 있기 때문에, 전처리 요건을 결정하기 위한 기초로서 성공적으로 이용될 수 있다. 일부 압축 툴에서, 상기 전처리 기능은 인코딩 처리 부분이다. 이외의 압축 툴에서, 소망하는 전처리가 압축 전에 수행된다.

판매를 위해 다운로드가능한 오디오 파일 이외에, 각 곡은 또한 곡이 LBR 스트리밍 프로토콜을 통해 샘플되도록 하는 저 비트 레이트(LBR) 인코딩된 클립을 갖는다. 상기 LBR 인코딩은 또한 콘텐츠 처리 툴(155)을 책임진다. 상기 클립은 분리 PCM 파일 또는 길이 및 오프셋의 파라미터로서 콘텐츠 제공자(들)(101)에 의해 제공된다.

워터마킹에서, 인코딩 툴은 DLL 또는 명령 라인 시스템 호출 인터페이스 및 전치를 및 압축을 위해 전달된 모든 필요한 파라미터를 통해 로드될 수 있다. 프론트 엔드 인코딩 툴은, 예컨대 콘텐츠가 음악이고, 곡의 장르가 소정의 오디오 전처리를 수행하기 전에 콘텐

트 공급자(들)의 데이터베이스(160)로부터 얻어진다고 결정되면, 메타 데이터 융합 및 엔트리 툴(161)로 동기화 요건을 갖을 수 있다. 이것은 선택된 인코딩 툴 및 곡에 대해 결정된 장르가 어떤 것인가에 따라 달라진다. 콘텐츠 제공자(들)(101)가 곡마다 인코딩된 품질 레벨의 선택을 변화시키면, 상기 정보는 또한 인코딩 단계 전에 제공되며, 메타 데이터 융합 및 엔트리 툴(161)에 의해 발생된 메타 데이터와 일치한다.

다양한 고품질 인코딩 알고리즘 및 툴이 최근 공개되었다. 이를 통해 프론트 인코딩 툴이 다양한 산업 인코딩 툴을 지원할 수 있다.

이제, 도 12를 참조하면, 본 발명에 따른 도 8의 자동 메타 데이터 취득 툴에 대한 일 실시예의 흐름도가 도시된다. 처리는 콘텐츠 제공자(들)(101)가 검사한 매체로부터 식별자를 판독하여 개시된다. 콘텐츠의 일례로서, 오디오 CD 실시예에서는, 다음의 코드들이 이용가능한 범용 가격 코드(UPC), 국제 표준 기록 코드(ISRC), 국제 표준 음악 번호(ISMN)일 수 있다. 상기 식별자는, 스텝 1201에서, 예컨대 오디오용 오디오 CD 플레이어, DVD 영화용 DVD 플레이어, DAT 녹음용 DAT 레코더 등의 콘텐츠용 전용 플레이어에서 판독된다. 다음에, 상기 식별자는 스텝 1202에서 콘텐츠 제공자(들)(101)에 대한 데이터베이스(160)를 인덱스하기 위해 이용된다. 스텝 1203에서, 도 8에 설명된 바와 같은 워크 플로우 처리에 필요한 정보의 일부 또는 모두가 데이터베이스(160) 및 소정의 다른 관련된 소스에서 검색된다. 상기 정보는 콘텐츠(113) 및 이와 관련된 메타 데이터를 포함할 수 있다. 스텝 1204에서, 검색된 부가 정보가 전자 콘텐츠(113)를 생성하기 위한 워크 플로우 관리자(154)를 개시하기 위해 이용된다. 여러 개의 오디오 CDS 같은 매체의 여러 개의 선택이, 자동 메타 데이터 취득 툴이 전자 배포용의 일련의 콘텐츠(113)를 생성할 수 있도록 큐될 수 있음이 이해되어야 한다. 예를 들면, 모든 콘텐츠(113)가 일련의 CDS로부터 생성되거나, 또는 콘텐츠 제공자(들)(101)에 의해 검사된 하나 이상의 CDS로부터 선택될 수 있다.

다른 실시예에서, 전처리 파라미터는 콘텐츠 제공자(들)의 데이터베이스(160)로부터 자동적으로 검색될 수 있다. 이하, 본 발명에 따른 도 8의 전처리 및 압축 툴의 전처리 및 압축 파라미터를 자동적으로 설정하기 위한 방법의 흐름도인 도 13을 참조한다. 본 실시예에서, 콘텐츠(113)는 음악이다. 스텝 1301에서, 음악(콘텐츠(113))은 콘텐츠 처리 툴(155)로 인코딩되도록 선택된다. 선택된 음악의 장르는 스텝 1302에서 결정된다. 이것은 도 12에서 설명된 처리로부터 검색된 부가 정보 같은 이용가능한 다른 메타 데이터를 이용하거나 또는 수동으로 기입될 수 있다. 이후, 스텝 1303에서, 오디오 압축 레벨 및 오디오 압축 알고리즘이 검사된다. 다음에, 스텝 1304에서, 어떤 압축 파라미터가 전처리 및 압축 처리(809)에서 이용되어야 하는가에 대하여 장르, 압축 설정 및 압축 알고리즘에 의한 참조가 이루어질 수 있다.

3. 콘텐츠 품질 제어 툴

콘텐츠 품질 제어 툴은 상술된 바와 같이 콘텐츠 품질 제어 처리(810)를 실행하기 위한 기능을 사용자에게 제공한다. 이것은 선택적 콘텐츠 처리 툴로서, 품질 제어 기술자가 인코딩 및 워터마크된 콘텐츠 파일을 검사할 기회를 제공하며, 품질 판단에 기초하여 콘텐츠 파일을 승인 또는 거부한다. 이들은 품질이 적당할 때까지 수동 처리 조정을 하여 콘텐츠를 재-인코딩하거나, 또는 재처리를 위해 곡을 플래그하여 문제를 설명한 주석을 첨부할 수 있다.

상기 처리 단계는 콘텐츠 처리 워크 플로우의 선택적 또는 필수적인 단계로서 콘텐츠 제공자(들)(101)에 의해 구성될 수 있다. 부가적인 선택적 최종 품질 보증 처리(813) 단계는 상기 콘텐츠에 대한 모든 SC(들)(예컨대, CD상의 곡에 대한 각 SC(들))를 패키징한 후 제공되며, 이때 콘텐츠 인코딩의 품질이 테스트되지만, 암호화 및 패키징 전에 문제를 포착하여 더 효율적인 콘텐츠 처리를 가능하게 한다. 따라서, 모든 처리가 최종적으로 완료될 때까지 대기하는 것과는 대조적으로 상기 단계에서 콘텐츠 품질이 보장되는 것이 매우 바람직하다.

4. 암호화 툴

암호화 툴은 상술된 바와 같이 암호화 처리(811)를 실행하기 위한 기능을 사용자에게 제공한다. 콘텐츠 암호화는 콘텐츠 처리 툴(155)의 최종 단계이다. 인코딩 툴에 의해 생성된 콘텐츠의 각 버전이 이제 암호화된다. 암호화 툴은 SC(들) 패커의 기능이다. SC(들) 패커는 곡을 암호화하기 위해 호출되며, 발생된 암호화 키 이용을 복귀시킨다. 이후, 상기 키는 메타 데이터 SC(들)(620)의 생성 시 이용하기 위하여 SC(들) 패커로 전달된다.

E. 콘텐츠 SC(들) 생성 툴

일단, 모든 메타 데이터가 수집되면, 콘텐츠 SC(들) 생성 툴은 이들이 의도한 이용에 기초하여 메타 데이터를 카테고리 그룹화한다. 상기 메타 데이터의 그룹은 SC(들) 패커 툴에 전달된 파일들에 메타 데이터 SC(들)(620)에 대한 메타 데이터 부문으로서 기입된다. 각 부문(파일)은 유일한 처리 요건을 갖는다. 일단, 연관된 곡이 처리되어 암호화되며, 타겟 목적지(콘텐츠 호스팅 사이트(들)(111)의 URL)가 결정되면, 콘텐츠(113)에 대한 콘텐츠 SC(들)(630)이 생성될 준비를 한다. 처리를 완료하고 상술된 모든 요건을 충족한 콘텐츠(113)는 워크 플로우 관리자(154)의 패커 큐에서 패키징을 위해 큐된다.

이제, 콘텐츠 SC(들) 생성 툴은 메타 데이터 융합 및 엔트리 툴(161)의 이전 단계에 의해 생성된 모든 필요한 파일들을 검색하고, 메타 데이터 SC(들)(620) 및 콘텐츠 SC(들)(630)을 생성하기 위한 SC(들) 패커 기능을 호출한다. 상기 처리에서는 각 곡마다 단일 메타 데이터 SC(들)(620) 및 다중 콘텐츠 SC(들)(630)을 생성한다. 예를 들어, 콘텐츠가 음악이면, 전 곡의 다양한 품질 레벨에 대한 오디오 처리중 생성된 오디오 파일들 각각이 독립적 콘텐츠 SC(들)(630)로 팩된다. 샘플 클립에 대하여 생성된 오디오 파일은 메타 데이터 SC(들)(620)에 포함될 메타 데이터 파일로서 전달된다.

F. 최종 품질 보증 툴

최종 품질 보증 툴은 상술된 바와 같이 최종 품질 보증 처리(813)를 실행하기 위한 기능을 사용자에게 제공한다. 일단, 모든 SC(들)

가 콘텐츠 파일마다 구축되면, 콘텐츠는 최종 품질 보증 검색을 위해 이용될 수 있다. 품질 보증은 여러 단계의 콘텐츠(113) 준비 처리로 수행될 수 있다. 콘텐츠 제공자(들)(101)는 각 주요한 단계가 이후에 과도한 재작업을 방지하기 위해 완료됨에 따라 품질 보증을 수행하기 위한 선택을 하거나, 또는 모든 오디오 준비 처리가 완료되어 동시에 모두에 품질 보증을 수행할 때까지 대기하기 위한 선택을 할 수 있다. 후자가 선택되면, 품질 보증은 SC(들)의 생성이 완료될 때 수행된다. 상기 틀은 곡에 대한 각 SC(들)가 열기, 심사 및 오디오 플레이될 수 있도록 한다.

소정의 문제가 발견되면, 작은 텍스트 변화라도 SC(들)의 내부 보안 특징으로 인해 SC(들)가 재구축되어야만 한다. 불필요한 재-처리 시간을 피하기 위해, 중간 품질 보증 단계가 메타 데이터의 정확도를 보장하기 위하여 이용되고, 특별한 품질 보증 단계가 상기 곡과 연관된 SC(들) 사이에서 적절한 교차 참고를 확인하기 위해 마련되도록 하는 것이 권장된다. 만약, 문제가 발생하면, 보증자는 곡에 첨부될 문제 설명을 기입하며, 이것을 재처리를 위해 적절한 처리 큐에 다시 큐시킨다. 상태는 곡의 모든 관련된 성분의 상태를 표시하기 위해 워크 플로우 관리자(154)에서 적절하게 갱신된다. 만약, 어떠한 문제도 발견되지 않으면, 콘텐츠(113)는 릴리즈를 위한 준비로서 마크 또는 플래그된다.

G. 콘텐츠 분산 틀

콘텐츠 분산 틀은 상술된 바와 같이 콘텐츠 분산 처리(184)를 실행하기 위한 기능을 사용자에게 제공한다. 일단, 콘텐츠(113)가 릴리즈를 위해 승인되면, 콘텐츠(113)에 대한 SC(들)는 콘텐츠 분산 처리의 큐에 배치된다. 콘텐츠 분산 틀은 큐를 모니터하고, 콘텐츠 제공자(들)(101)에 의해 제공된 구성 설정에 기초하여 SC(들) 파일 그룹의 일괄 전달, 또는 SC(들) 파일의 즉시 전달을 수행한다. 콘텐츠 제공자(들)(101)는 또한 이들이 릴리즈를 위해 수동으로 플래그될 때까지 상기 큐에서의 모든 SC(들)을 자동적으로 홀드하기 위하여 콘텐츠 분산 틀을 선택적으로 구성할 수 있다. 이것은 콘텐츠 제공자(들)(101)가 그들의 스케줄된 날짜에 앞서 콘텐츠를 준비할 수 있도록 하며, 이들이 예컨대 새로운 곡, 영화 또는 게임을 릴리즈하고자 할 때까지 이들을 홀드한다. SC(들)는 또한 규정된 릴리즈 날짜에 기초하여 콘텐츠(113)로의 액세스를 제어할 수 있으며, 그래서 SC(들)의 전달을 실질적으로 홀드하기 위한 콘텐츠 제공자(들)(101)에 대한 요건이 없지만, 상기 수동 릴리즈 옵션은 아직 상기 목적을 위해 이용되거나, 또는 상기 큰 파일을 전달하기 위해 필요한 네트워크 대역폭을 관리하기 위해 이용될 수 있다.

릴리즈를 위해 플래그될 때, 콘텐츠(113)에 대한 콘텐츠 SC(들)(630)는 FTP를 통해 지시된 콘텐츠 호스팅 사이트(들)(111)에 전송된다. 메타 데이터 SC(들)(620)는 FTP를 통해 콘텐츠 프로모션 웹 사이트(156)에 전송된다. 여기서, SC(들)는 이들이 처리될 때까지 새로운 콘텐츠(113) 디렉토리로 스테이지되고, 콘텐츠 프로모션 웹 사이트(156)로 통합된다.

도 17은 본 발명에 따른 도 8의 자동 메타 데이터 취득 틀에 대한 부가 정보를 자동적으로 검색하기 위한 다른 실시예의 흐름도이다. 처리는 상기 도 8에서 설명된 것과 유사하다. 그러나, 감시 릴리즈(806)의 품질 검사 및 콘텐츠 품질 제어(809)는 품질 제어(1704)를 호출하여 하나의 품질 검사로 결합된다. 메타 데이터 SC 생성(807) 및 콘텐츠 SC 생성(812) 전에 품질 검사를 수행한다. SC 생성 전에 품질 검사를 수행하여, 콘텐츠(113) 및 연관된 메타 데이터 SC(들)(620)를 언패킹하는 단계를 제거한다. 또한, 본 실시예에서, 저작물 대기 활동/정보(801)의 큐는 제거된다. 작업은 활동이 요구됨에 따라 특별한 처리 큐상에 배치된다. 예를 들어, 작업이 수동 메타 데이터, 즉 기입될 부가적 메타 데이터를 필요로 하는 경우, 작업은 수동 메타 데이터 엔트리 큐상에 배치된다. 또한, 자동 메타 데이터 취득(803)은 메타 데이터 융합 및 엔트리 틀(161)과 콘텐츠 처리 틀(155) 이전에 앞서서 발생하기 위하여 새로운 콘텐츠 요구와 합치된다. 결국, 사용 조건(804)이 자동 메타 데이터 취득(803)시 및 수동 메타 데이터 엔트리(803)중 모두에서 기입되도록 지시하는 것이 중요하다. 그 이유는, 많은 사용 조건이 자동 메타 데이터 취득(803) 단계중에 자동적으로 채워질 수 있기 때문이다.

h. 콘텐츠 프로모션 웹 사이트

콘텐츠 제공자(들)(101)가 디지털 다운로드를 통해 판매에 이용가능한 정보를 가장 효과적으로 분산시키며, 고객에게 다운로드시키기 위해 이용될 수 있는 콘텐츠(113)를 작성할 수 있도록 하기 위해 전자 디지털 콘텐츠 스토어(들)(103)에 필요한 파일들을 취하기 위하여, 각 콘텐츠 제공자(들)(101)는 상기 정보를 하우징하는 보안 웹 사이트를 갖춰야 한다. 이것은 소매상 및 이러한 정보를 필요로 하는 다른 사람에게 이용될 수 있는 프로모션형 콘텐츠를 작성하기 위하여 일부 콘텐츠 제공자(들)(101)에 의해 최근에 이용되는 방법과 유사하다. 이러한 타입의 서비스가 이미 존재하는 경우에, 전자 디지털 콘텐츠 스토어(들)(103)가 다운로드를 통한 판매를 위해 이용될 수 있는 콘텐츠의 리스트를 볼 수 있는 웹 사이트에 부가적인 섹션이 부가될 수 있다.

콘텐츠 제공자(들)(101)는 상기 사이트의 레이아웃 및 디자인상에서 제어를 완료하거나, 또는 보안 디지털 콘텐츠 전자 배포 시스템(100)용 툴 키트 부분으로 제공된 터키 웹 서버 솔루션을 이용하기 위한 선택을 할 수 있다. 상기 서비스를 위한 자체의 디자인을 실시하기 위하여, 콘텐츠 제공자(들)(101)는 그들의 사이트를 액세스하는 전자 디지털 콘텐츠 스토어(들)(103)에 대한 메타 데이터 SC(들)(620)로의 링크를 제공하기만 하면 된다. 이것은 보안 디지털 콘텐츠 전자 배포 시스템(100)용 툴 키트를 이용하여 구현된다. 선택 처리 및 어떠한 정보가 도시되었는가에 따라 콘텐츠 제공자(들)(101)를 분별한다.

콘텐츠 분산 틀로부터 FTP를 통해 새로운 콘텐츠 디렉토리에 수신된 메타 데이터 SC(들)(620)는 콘텐츠 프로모션 웹 사이트(156)에 의해 처리된다. 상기 콘텐츠이너는 콘텐츠이너로부터 정보를 추출하거나 디스플레이하기 위하여 SC(들) 미리 보기 틀로 열릴 수 있다. 이후, 상기 정보는 HTML 웹 페이지를 갱신하거나, 및/또는 상기 서비스에 의해 유지되는 서치가능한 데이터베이스에 정보를 부가하기 위하여 이용될 수 있다. SC(들) 미리 보기 틀은 실제로 메타 데이터 SC(들)(620)를 열어서 처리하기 위해 전자 디지털 콘텐츠 스토어(들)(103)에 의해 이용되는 콘텐츠 취득 틀의 일부이다. 더 상세한 설명을 위하여 콘텐츠 취득 틀 섹션을 살펴본다. 이때, 메타 데이터 SC(들)(620) 파일은 콘텐츠 프로모션 웹 사이트(156)에 의해 유지되는 영구 디렉토리로 이동되어야 한다.

일단, 메타 데이터 SC(들)(620)가 콘텐츠 프로모션 웹 사이트(156)로 통합되면, 그 이용도가 공표된다. 콘텐츠 제공자(들)(101)는 각 새로운 메타 데이터 SC(들)(620)가 사이트에 부가됨에 따라 모든 가입 전자 디지털 콘텐츠 스토어(들)(103)에게 통지를 보내거나, 또는 그 날(또는, 주기) 부가된 모든 메타 데이터 SC(들)(620)의 일간(또는, 소정의 규정된 주기로) 단일 통지를 수행할 수 있다. 상기

통지는 부가된 메타 데이터 SC(들)(620)를 참조하는 파라미터를 포함한 규정된 CGI 스트링을 전송함으로써 전자 디지털 콘텐츠 스토어(들)(103) 웹 서버와 교환하는 표준 HTTP를 통해 수행된다. 상기 메시지는 이후에 설명되는 전자 디지털 콘텐츠 스토어(들)(103)의 통지 인터페이스 모듈에 의해 관리된다.

1. 콘텐츠 호스팅

오락 산업에서는 현재 이용되고 있는 수 만개의 콘텐츠 타이틀에 부가하여 해마다 CDS, 영화 및 게임 같은 수 천개의 콘텐츠 타이틀을 제작한다. 보안 디지털 콘텐츠 전자 배포 시스템(100)은 최근 스토어에서 이용될 수 있는 모든 콘텐츠 타이틀을 지원하기 위해 디자인된다. 보안 디지털 콘텐츠 전자 배포 시스템(100)이 언제나 하루를 기준으로 고객에게 다운로드할 수 있는 콘텐츠 타이틀의 수는 수 천 또는 수 만개이다. 이때, 엄청난 수의 타이틀에 대해서 엄청난 양의 대역폭이 필요하게 된다. 컴퓨터 디스크 공간 및 대역폭은 다중 콘텐츠 호스팅 사이트(들)(111)로 배포를 위한, 가능한 실행을 위해 호출을 필요로 한다. 시스템은 또한 전세계의 모든 고객을 지원한다. 이때, 글로벌한 고객으로의 고속 전달을 위한 해외 사이트를 필요로 한다.

보안 디지털 콘텐츠 전자 배포 시스템(100)에서 호스팅한 콘텐츠는 콘텐츠 제공자(들)(101)가 자신의 콘텐츠(113)를 호스팅하거나 또는 공동 설비 또는 설비의 세트를 공유할 수 있도록 디자인된다.

보안 디지털 콘텐츠 전자 배포 시스템(100)에서 호스팅한 콘텐츠는, 보안 디지털 콘텐츠 전자 배포 시스템(100)에 의해 제공된 모든 콘텐츠(113)를 집합적으로 포함한 다중 콘텐츠 호스팅 사이트(들)(111), 및 콘텐츠 제공자(들)(101)에 의해 제공된 현재의 핫 히트를 포함한 여러 개의 보조 콘텐츠 사이트(도시되지 않음)로 구성된다. 콘텐츠 호스팅 사이트(들)(111)의 수는 시스템을 이용하는 최종 사용자(들)의 수에 따라 변화된다. 보조 콘텐츠 사이트는 제한된 수의 곡을 호스트하지만, 이들은 시스템에서 이용될 확률이 높은 대역폭을 나타낼 수 있다. 보조 사이트는 주 사이트에서의 볼륨이 최대 용량 포인트까지 증가함에 따라 라인상에 도입된다. 보조 사이트는 다운로드 시간의 고속화를 돕는 네트워크 액세스 포인트(NAP)에 가까이 위치될 수 있다. 이들은 또한 다운로드 시간을 높이기 위하여 세계 도처의 다른 지형적 지역에 배치될 수 있다.

콘텐츠 제공자(들)(101)가 자체의 시스템에서 그들의 모든 콘텐츠(113)를 호스트하기 위한 선택을 하면, 이들은 부가적인 보조 콘텐츠 사이트를 갖거나 또는 갖지 않을 수 있는 단일 콘텐츠 호스팅 사이트(111)로서 작용할 수 있다. 이것은 이들이 자체의 가능한 배포 시스템을 구축할 수 있도록 하는 것이다. 다른 실시예에서, 전자 디지털 콘텐츠 스토어(들)(103)는 또한 소정의 콘텐츠(113)에 대한 콘텐츠 호스팅 사이트(들)(111)로서 작용할 수 있다. 상기 실시예에서는 전자 디지털 콘텐츠 스토어(들)(103) 및 콘텐츠 제공자(들)(101) 사이의 특별한 금융적 동의를 필요로 한다.

1. 콘텐츠 호스팅 사이트

콘텐츠(113)는, 본 명세서의 콘텐츠 제공자(들) 섹션에서 설명된 콘텐츠 분산 틀에 의해 FTP 또는 HTTP를 통해서, 또는 테이프, CD ROM, 플래시 또는 다른 컴퓨터 판독가능 매체상으로의 콘텐츠 전달 같은 오프라인 수단을 통해 콘텐츠 호스팅 사이트(들)(111)에 부가된다. 콘텐츠 제공자(들)(101)에 의해 생성된 메타 데이터 SC(들)(620)는 상기 콘텐츠(113)에 대한 콘텐츠 SC(들)(630)를 위치시키는 URL을 나타내는 필드를 포함한다. 상기 URL은 콘텐츠 호스팅 사이트(들)(111)에 대응한다. 전자 디지털 콘텐츠 스토어(들)(103)는, 오퍼 SC(들)(641) 내의 콘텐츠 제공자(들)(101)에 의해 허용된다면 상기 URL을 무시할 수 있다. 최종 사용자 장치(들)(109)는 이들이 콘텐츠 SC(들)(630)를 다운로드 하고자 할 때, 상기 콘텐츠 호스팅 사이트(들)(111)와 통신한다.

최종 사용자 장치(들)(109)는 인가 SC(들)(660)를 콘텐츠 호스팅 사이트(들)(111)에 전송함으로써 콘텐츠 SC(들)(630)에 대한 요구를 개시한다. 이것은 클리어링하우스(들)(105)에 의해 복귀된 것과 동일한 인가 SC(들)(660)이다. 인가 SC(들)(660)의 디지털 기호는 유효한 인가 SC(들)(660)인가를 판단하기 위하여 검증될 수 있다. 만약, 유효한 인가 SC(들)(660)라면, 다운로드가 개시되거나, 또는 다운로드 요구가 다른 콘텐츠 호스팅 사이트(들)(111)에 재지시될 수 있다.

2. 보안 디지털 콘텐츠 전자 배포 시스템(100)에 의해 제공된 콘텐츠 호스팅 사이트(들)

보안 디지털 콘텐츠 배포 시스템(100)에서, 사이트가 콘텐츠(113)를 다운로드하기 위하여 이용되어야 하는 가의 결정은 콘텐츠 SC(들)(630)에 대한 개시 요구를 수신받은 주 콘텐츠 사이트에 의해 이루어진다. 상기 사이트는 이러한 결정을 하기 위하여 다음의 정보를 이용한다:

- 요구된 콘텐츠(113)를 호스트하는 보조 콘텐츠 사이트가 있는가? (보안 디지털 콘텐츠 전자 배포 시스템(100)에 의해 제공된 콘텐츠(113)의 대부분은 주 사이트에만 위치됨); 최종 사용자 장치(들)(109)가 지형적으로 어느 것에 위치되는가? (상기 정보는 요구가 최종 사용자 장치(들)(109)에서 개시될 때, 최종 사용자 장치(들)(109)로부터 얻어질 수 있으며, 이것은 클리어링하우스(들)(105)에 오퍼 SC(들)(650)로 전달됨); 적절한 보조 사이트가 나타나며 유효한가? (종종, 보조 사이트는 오프라인일 수 있음); 보조 사이트의 로드가 어떠한가? (일부 경우, 보조 사이트가 보다 덜 혼잡한 활동성의 다른 사이트로 스왑되는 곳으로 선택될 수 있음).

콘텐츠 SC(들)(630)를 최종 사용자 장치(들)(109)에 전송하기 전에, 최종 사용자의 요구에 대한 분석 및 검증이 수행된다. 데이터베이스에는 콘텐츠(113)를 다운로드하기 위해 이용된 모든 인가 SC(들)이 보존된다. 이러한 데이터베이스는 최종 사용자 장치(들)(109)가 구매한 콘텐츠(113)의 각 피스에 대하여 한번의 요구만을 보증하기 위하여 검색될 수 있다. 이것은 부당한 사용자가 콘텐츠 호스팅 사이트(들)(111)의 속도를 늦출 목적으로 콘텐츠 호스팅 사이트(들)(111)에 반복적으로 액세스하는 것을 방지하며, 콘텐츠 SC(들)(630)의 비인증된 다운로드를 방지한다.

보조 콘텐츠 사이트로의 콘텐츠(113)의 프로모션 및 디모션은 콘텐츠(113)의 개별 피스마다의 고객 요구에 기초하여 주기적으로 수행된다.

콘텐츠 호스팅 라우터(Router)콘텐츠 호스팅 라우터(도시되지 않음)는 콘텐츠 호스팅 사이트(들)(111)에 위치하며, 콘텐츠(113)를 다운로드하고자 하는 최종 사용자(들)로부터의 모든 요구를 수신한다. 이것은 이들이 콘텐츠(113)를 실제로 구입하였는가를 보증하기 위하여 최종 사용자(들) 요구의 유효성 검사를 수행한다. 데이터베이스는 어떤 콘텐츠(113)가 이들에 위치되는가와 그 현재 상태를 포함한 보조 콘텐츠 사이트의 상태로 유지된다. 이 현재의 상태는 사이트에서의 활동량과 사이트가 유지를 위해 다운되는가의 여부를 포함한다.

콘텐츠 호스팅 라우터와의 유일한 인터페이스는 콘텐츠(113)가 다운로드될 필요가 있을 때, 최종 사용자 장치(들)(109)에 의해 전송된 인가 SC(들)(660)이다. 인가 SC(들)(660)는 사용자에게 콘텐츠(113)의 다운로드가 허용됨을 표시하는 정보를 포함한다.

보조 콘텐츠 사이트보조 콘텐츠 사이트(도시되지 않음)는 보안 디지털 콘텐츠 배포 시스템(100)의 대중적인 콘텐츠(113)를 호스팅한다. 상기 사이트는 전세계에 걸쳐 지형적으로 분산되며, 다운로드 시간을 향상시키기 위하여 인접 네트워크 액세스 포인트(NAP)에 위치된다. 상기 사이트는 주 콘텐츠 호스팅 사이트(들)(111)에서의 요구가 최대 용량에 가까와짐에 따라 시스템에 부가된다.

IX. 전자 디지털 콘텐츠 스토어(들)

A. 개요 - 다중 전자 디지털 콘텐츠 스토어(들)(103)를 위한 지원

전자 디지털 콘텐츠 스토어(들)(103)는 근본적으로 소매상이다. 이들은 고객에게 배포될 콘텐츠(113)를 마켓하는 엔티티이다. 콘텐츠(113)의 배포를 위하여, 이것은 디지털 콘텐츠 소매 웹 사이트, 디지털 콘텐츠 소매 스토어 또는 고객에게 전자 콘텐츠(113)를 마케팅 시 수반되는 소정의 사업을 포함할 수 있다. 이 사업자는 단지 전자 콘텐츠(113)의 판매만을 마켓하거나, 또는 이들이 현재 어떠한 제품의 판매를 제공하든지 간에 전자적 상품의 판매를 추가하기 위한 선택을 할 수 있다. 다운로드 가능한 전자 상품을 전자 디지털 콘텐츠 스토어(들)(103)의 서비스 제공에 도입하는 것은 보안 디지털 콘텐츠 전자 배포 시스템(100)의 일부로서 전자 디지털 콘텐츠 스토어(들)(103)를 위해 개발된 툴 세트를 통해 구현된다.

상기 툴들은 다음의 것들을 전자 디지털 콘텐츠 스토어(들)(103)에 의해 이용된다: • 콘텐츠 제공자(들)(101)에 의해 패키징된 메타 데이터 SC(들)(620)를 얻기 위하여, • 그들의 서비스 제공을 구축하기 위한 입력으로 이용될 상기 SC(들)로부터 콘텐츠(113)를 추출하기 위하여, • 이들이 판매를 위해 제공하고 있는 다운로드 가능한 콘텐츠(113)를 설명하는 오퍼 SC(들)(641)를 생성하기 위하여, • 트랜잭션 SC(들)(640)를 생성하여 최종 사용자(들)(109)에게 전송함으로써 판매의 승인 및 다운로드의 개시를 처리하기 위하여, • 다운로드 가능한 콘텐츠(113) 판매의 트랜잭션 로그 및 각 다운로드의 상태를 관리하기 위하여, • 상태 통지 및 트랜잭션 인증 요구를 처리하기 위하여, • 회계 조정을 수행하기 위하여 툴은 전자 디지털 콘텐츠 스토어(들)(103)가 어떻게 다운로드 가능한 전자 콘텐츠(113)의 판매를 그 서비스에 통합하고자 하더라도 유연성을 주기 위하여 디자인된다. 툴은 구매된 다운로드 가능한 콘텐츠(113)에 대한 모든 금융 결제가 비를 이것이 필요하지 않더라도 클리어링하우스(들)(105)에 의해 처리되는 요구와 같은 방식으로 이용될 수 있다. 상기 툴은 또한 전자 디지털 콘텐츠 스토어(들)(103)가 프로모션 및 특별한 오퍼의 제공을 포함하여 그들의 고객에게 완전하게 서비스하며 자체적으로 금융 트랜잭션을 처리할 수 있도록 한다. 상기 툴은 전자 디지털 콘텐츠 스토어(들)(103)가 다운로드 가능한 콘텐츠(113)의 판매를 그 현존 서비스에 신속히 통합시킬 수 있도록 한다. 또한, 전자 디지털 콘텐츠 스토어(들)(103)는 다운로드 가능한 콘텐츠(113)를 반드시 호스팅할 필요가 없으며, 그 분산을 관리하지 않는다. 상기 기능은 콘텐츠 제공자(들)(101)에 의해 선택된 콘텐츠 호스팅 사이트(들)(111)에 의해 수행된다.

전자 디지털 콘텐츠 스토어(들)(103)용 툴은 양호한 실시예에서는 자바로 실행되지만, C/C++, 어셈블러 같은 다른 프로그래밍 언어가 이용될 수 있다. 전자 디지털 콘텐츠 스토어(들)(103)에 대하여 이하에 설명되는 툴들이 다양한 하드웨어 및 소프트웨어 플랫폼상에서 실행될 수 있음이 이해되어야 한다. 완전한 시스템 또는 그 구성 성분중 일부로서의 전자 디지털 콘텐츠 스토어(들)(103)는 웹 또는 플로피 디스켓, CD ROM 및 이동가능한 하드디스크 드라이브 같은 전자 배포물을 포함한, 그러나 이들에 한정되지 않는 컴퓨터 판독가능 매체에서의 애플리케이션 프로그램으로 배포될 수 있다.

다른 실시예에서, 전자 디지털 콘텐츠 스토어(들)(103)의 성분은 프로그래머의 소프트웨어 툴 키트의 일부이다. 이 툴 키트는 이하에 설명되는 툴과 포괄적 전자 디지털 콘텐츠 스토어(들)(103) 성분들과의 규정된 인터페이스를 가능하게 한다. 상기 규정된 인터페이스는 API, 즉 애플리케이션 프로그램 인터페이스의 형태이다. 상기 API를 이용하는 개발자는 고레벨 애플리케이션으로부터의 성분의 소정의 기능을 실행할 수 있다. API를 상기 성분에 제공함으로써, 프로그래머는 상기 성분중 일부의 자원 및 상기 기능을 재생성할 필요없이 개별화된 전자 디지털 콘텐츠 스토어(들)(103)를 신속히 개발할 수 있다.

전자 디지털 콘텐츠 스토어(들)(103)는 웹 기반의 서비스 제공에 제한되지 않는다. 제공된 툴은 상기 콘텐츠(113)를 최종 사용자(들)에게 전달하기 위해 이용되는 전달 모드 또는 전송 기반시설에 관계없이 다운로드 가능한 전자 콘텐츠(113)를 판매하고자 하는 모든 전자 디지털 콘텐츠 스토어(들)(103)에 의해 이용된다. 위성 및 케이블 기반시설상에서 제공된 방송 서비스는 또한 취득, 패키지 및 전자 콘텐츠(113) 판매 추적을 위해 상기와 같은 툴을 이용한다. 상기 오퍼가 최종 사용자(들)에 전달되는 방법 및 판매를 위한 전자 제품의 표시는 방송 기반의 서비스 제공 및 포인트 투 포인트 상호작용 웹 서비스 타입 제공간의 주요한 차이점이다.

B. 포인트 투 포인트 전자 디지털 콘텐츠 배포 서비스

포인트 투 포인트는 주로 전자 디지털 콘텐츠 스토어(들)(103)와 최종 사용자 장치(들)(109)간의 일대일 상호작용 서비스를 의미한다. 이것은 일반적으로 전화나 케이블 모뎀 접속 같이 제공된 인터넷 웹 기반의 서비스를 나타낸다. 인터넷이외의 네트워크는 이들이 웹 서버/클라이언트 브라우저 모델과 일치하는 한 상기 모델에서 마찬가지로 지원된다. 도 9는 전자 디지털 콘텐츠 스토어(들)(103)의 처리, 주요 툴 및 성분을 예시한 블록도이다.

1. 통합 요건

보안 디지털 콘텐츠 전자 배포 시스템(100)은 새로운 온라인 사업을 창조할 뿐만 아니라 다운로드 가능한 전자 콘텐츠(113)의 판매를 그들의 현재 재고에 통합시키기 위한 방법을 기존의 사업자에게 제공한다. 전자 디지털 콘텐츠 스토어(들)(103)에 제공된 툴들의 세트는 상기 통합 노력을 줄일 수 있다. 콘텐츠 취득 툴(171) 및 SC(들) 패커 툴(153)은, 참여 콘텐츠 제공자(들)(101)로부터 판매를 위해 이용될 수 있는 정보를 취득하고, 상기 다운로드 가능한 객체를 자체의 재고로서 조회하기 위해 필요한 파일을 생성하기 위한 방법을 전자 디지털 콘텐츠 스토어(들)(103)에 제공한다. 이러한 처리는 일괄 구동되며, 상당히 자동화될 수 있으며, 새로운 콘텐츠(113)를 사이트에 통합하기 위해서만 실행될 수 있다.

보안 디지털 콘텐츠 전자 배포용 툴은, 전자 다운로드 가능한 콘텐츠(113)의 판매를 웹 기반의 전자 디지털 콘텐츠 스토어(들)(103) (즉, 콜롬비아 하우스 온라인, 불러바드, @타워)로, 및 최소의 변화를 갖는 대등한 것을 패러다임을 소매하는 이들의 현재 콘텐츠(113)에 통합시킬 수 있도록 디자인된다. 여러 가지의 통합 방법들이 가능하며, 양호한 실시예에서, 전자 디지털 콘텐츠 스토어(들)(103)는 모든 제품 서치, 미리 보기, 선택(쇼핑 카트) 및 구매를 위한 지원을 제공한다. 각 전자 디지털 콘텐츠 스토어(들)(103)는 고객과의 고객 충실도를 확립하고, 자체의 인센티브를 지속적으로 제공하며, 그 저작물을 최근에 하는 것과 같이 마켓한다. 보안 디지털 콘텐츠 전자 배포 시스템(100)에서는, 단순히 그 재고에서의 저작물이 또한 전자 다운로드를 위해 이용될 수 있음을 나타내고, 그 고객이 구매 선택을 할 때 전자 다운로드 옵션을 선택하도록 하면 된다. 다른 실시예에서, 고객의 쇼핑 카트는 전자(콘텐츠(113))와 물리적 매체 선택의 혼합을 포함할 수 있다. 고객이 체크 아웃하고, 전자 디지털 콘텐츠 스토어(들)(103)가 구매된 물리적 제품을 처리하기 위한 적하 및 조정 기능을 로그 또는 통지 및 금융 결제를 완료한 후, 전자 디지털 콘텐츠 스토어(들)(103)의 상거래 관리 기능이 모든 전자 다운로드를 관리하기 위해 트랜잭션 처리기 모듈(175)을 호출한다. 단순히 보안 디지털 콘텐츠 전자 배포 시스템(100)용 툴 키트에 의해 관리된 시점에서 필요한 정보 및 모든 처리를 전달한다. 다른 실시예에서, 트랜잭션 관리의 다른 방법들이, 또한 전자 디지털 콘텐츠 스토어(들)(103)가 다운로드 가능한 제품만을 팔고자 할 때의 금융 결제를 조정하거나, 또는 물리적인 것과 다운로드 가능한 제품의 금융 결제를 분리하기 위하여 보안 디지털 콘텐츠 전자 배포 시스템(100)용 툴을 이용하는 것이 가능하다.

제품의 다운로드를 관리하기 위하여, 전자 디지털 콘텐츠 스토어(들)(103)에 콘텐츠 제공자(들)(101)용 콘텐츠 프로모션 웹 사이트(156)로부터 취득한 각 다운로드 가능한 저작물에 대한 저작물 ID(도시되지 않음)가 주어진다. 이 저작물 ID는 다운로드 가능한 저작물의 고객의 구매 선택과 연관된다. 저작물 ID는 전자 디지털 콘텐츠 스토어(들)(103)가 사용자가 구매한 저작물을 식별하기 위해 트랜잭션 처리기 모듈(175)에 전달한 것이다. 저작물을 설명하기 위하여 생성된 SC(들)(오퍼-SC(들)(641))는 전자 디지털 콘텐츠 스토어(들)(103)로부터 분리되며 전자 디지털 콘텐츠 스토어(들)(103)에 투명하게 그들의 존재를 만들고 상기 객체의 관리를 단순화하기 위한 노력으로 오퍼 데이터베이스(181)에 보존된다.

트랜잭션 처리기 모듈(175) 및 다른 부가 기능은 DLL 또는 C 객체 라이브러리에 웹 서버측의 실행가능한 (즉, CGI 및 NSAPI, ISAPI 호출가능 기능) 또는 간단한 API로서 제공된다. 상기 기능은 클리어링하우스(들)(105)와의 선택적 상호작용 및 최종 사용자(들) 상호작용을 위한 실행 시간 처리를 관리한다. 상기 기능은 콘텐츠(113) 다운로드 처리를 개시하기 위해 필요한 파일을 생성하여 최종 사용자 장치(들)(109)에 다운로드하기 위한 웹 서버의 상거래 서버와 상호작용한다. 이들은 또한 인증을 제공하기 위해 선택적 상호작용을 관리하고, 활동의 완료를 통지받는다.

회계 조정 툴(179)은 또한 클리어링하우스(들)(105)의 트랜잭션 로그 및 자체에 기초하여 회계를 조정하기 위해 클리어링하우스(들)(105)와의 계약시 전자 디지털 콘텐츠 스토어(들)(103)을 지원하기 위하여 제공된다.

2. 콘텐츠 취득 툴(171)

콘텐츠 취득 툴(171)은 메타 데이터 SC(들)(620)를 미리 보고 다운로드하기 위해 콘텐츠 프로모션 웹 사이트(156)와의 인터페이스를 역할을 한다. 콘텐츠 프로모션 사이트는 표준 웹 사이트이기 때문에, 웹 브라우저는 상기 사이트를 항해하기 위해 전자 디지털 콘텐츠 스토어(들)(103)에 의해 이용된다. 항해의 특징은 콘텐츠 제공자(들)(101)의 사이트 디자인에 기초하여 변화된다. 일부 사이트들은 많은 스크린의 프로모션 정보를 고가의 서치 자격에 제공할 수 있다. 이외의 사이트들은 타이틀 리스트, 가수 또는 이로부터 선택된 새로운 릴리즈를 갖는 단순한 브라우저 인터페이스를 갖을 수 있다. 모든 사이트들은 곡 또는 앨범의 모든 프로모션적, 설명적 정보를 포함한 메타 데이터 SC(들)(620)의 선택을 포함한다.

또한, 전자 스토어(103)는 콘텐츠 갱신에 동의하고 FTP를 통해 자동으로 갱신을 수신할 수 있다.

메타 데이터 보기 콘텐츠 취득 툴(171)은 메타 데이터 SC(들)(620) 링크가 콘텐츠 프로모션 웹 사이트(156)에서 선택될 때마다 착수하는 웹 브라우저 헬퍼 애플리케이션이다. SC(들)의 선택은 이것이 전자 디지털 콘텐츠 스토어(들)(103)에 다운로드되도록 하여 헬퍼 애플리케이션을 착수시킨다. 콘텐츠 취득 툴(171)은 메타 데이터 SC(들)(620)를 열고, 여기에 포함된 암호화된 정보를 디스플레이한다. 디스플레이된 정보는 음악의 예에서 곡과 연관된 그래픽 이미지(들) 및 곡을 설명하는 정보 같은 추출된 메타 데이터(173)를 포함하며, 곡의 미리 보기 클립은 또한 메타 데이터 SC(들)(620)에 포함되는 경우에 들릴 수 있다. 콘텐츠(113)가 음악인 예에서, 곡 또는 앨범, 앨범 타이틀 및 가수 같은 프로모션형 정보는 또한 콘텐츠 제공자(들)(101)에 의해 제공된 경우에 도시된다. 이러한 정보는 브라우저 윈도우에서 일련의 링크된 HTML 페이지로 디스플레이된다. 곡 및 가사 같은 구매가능한 콘텐츠(113) 및 콘텐츠 제공자(들)(101)가 보호받기를 원하는 어떠한 다른 메타 데이터도 상세 콘텐츠 웹 사이트(180)에 액세스될 수 없다.

다른 실시예에서, 콘텐츠 제공자(들)(101)는 유료용의 선택적 프로모션 콘텐츠를 제공한다. 본 실시예에서, 상기 프로모션형 콘텐츠는 메타 데이터 SC(들)(620)로 암호화된다. 상기 데이터를 열기 위한 금융 결제는 지정된 요금으로 과금된 전자 디지털 콘텐츠 스토어(들)(103)를 위한 회계를 갖는 클리어링하우스(들)(105)를 통해 관리될 수 있다.

메타 데이터 추출미리 보기 자격 이외에, 상기 툴은 메타 데이터 추출 및 오퍼 SC(들)(641) 준비의 두 가지 부가적 특징을 제공한다.

메타 데이터 추출 옵션의 선택으로 메타 데이터가 저장된 경로 및 파일명을 기입하기 위해 전자 디지털 콘텐츠 스토어(들)(103)를 프롬프트한다. 텍스트 메타 데이터는 상세 콘텐츠 웹 사이트(180)가 그 데이터베이스에 수입될 수 있는 ASCII로 정해진 텍스트 파일로 저장된다. ASCII로 정해진 파일은 또한 독립 TOC 파일로 생성된다. 부가적 옵션이 다른 국제 언어 지원(NLS)으로 지원된 포맷으로 추출하기 위해 이용될 수 있다.

추출된 데이터에 제공된 한 가지 중요한 정보는 저작물 ID이다. 이 저작물 ID는 전자 디지털 콘텐츠 스토어(들)(103)를 위한 상거래 관리 기능이 트랜잭션 처리기 모듈(175)(더 많은 정보는 트랜잭션 처리 섹션에서 언급됨), 사용자가 구매한 콘텐츠(113)를 식별하기 위해 필요한 것이다. 트랜잭션 모듈(175)은 최종 사용자 장치(들)(109)로의 이어지는 다운로드를 위해 오퍼 데이터베이스(181)로부터 적절한 오퍼 SC(들)(641)를 정당하게 검색하기 위해 상기 저작물 ID를 이용한다. 전자 디지털 콘텐츠 스토어(들)(103)는 그 사이트에 다운로드 가능한 콘텐츠(113)의 오퍼가 어떻게 나타나는가에 따라 완전 제어를 한다. 보안 디지털 콘텐츠 전자 배포 시스템(100)용 툴과의 정당한 인터페이스를 위해 상기 저작물 ID에 제공된 콘텐츠(113)의 교차 참조를 실행하기만 하면 된다. 여기서 상기 정보를 제공하여, 전자 디지털 콘텐츠 스토어(들)(103)가 오퍼 SC(들)(641)와 병렬로 그 재고 및 판매 페이지(데이터베이스)로 상기 저작물 또는 콘텐츠(113)를 통합하도록 할 수 있는데, 그 이유는 두 가지 처리 모두가 저작물을 참조하기 위해 동일한 저작물 ID를 이용하기 때문이다. 이것은 이하에 다시 설명된다.

오퍼 SC(들) 생성 패커(153)전자 디지털 콘텐츠 스토어(들)(103)는 판매를 위한 다운로드 가능한 콘텐츠(113)를 설명하는 오퍼 SC(들)(641)를 생성해야 한다. 오퍼 SC(들)(641)로 향하는 정보의 대부분은 메타 데이터 SC(들)(620)로부터 유도된다. 콘텐츠 취득 툴(171)은 다음에 의해 오퍼 SC(들)를 생성한다:

· 메타 데이터 SC(들)(620)에서의 오퍼 SC(들) 템플릿에 의해 규정된 바와 같이 오퍼 SC(들)(641)에 포함될 필요가 없는 메타 데이터 SC(들)(620)로부터의 부분들을 제거함으로써 · 전자 디지털 콘텐츠 스토어(들)(103)용의 상기 툴에서의 구성 옵션에 의해 지정된 디폴트에 의해 규정된 바와 같이 부가적 필요 부분들을 부가함으로써 · 메타 데이터 SC(들)(620)에서의 오퍼 SC(들) 템플릿에 의해 규정된 바와 같이 부가적 필요 입력 및 선택에 대한 프롬프팅을 함으로써 · 상기 정보를 SC(들) 포맷으로 펌하기 위해 SC(들) 패커(153)를 호출함으로써 최종 사용자 장치(들)(109)상에 플레이어 애플리케이션(195; 이후에 다시 설명됨)에 의해 디스플레이될 메타 데이터는 메타 데이터 SC(들)(620)에 보존된다. 그 웹 서비스 데이터베이스로의 입력으로서 전자 디지털 콘텐츠 스토어(들)(103)에 의해서만 이용된 다른 프로모션 메타 데이터는 메타 데이터 SC(들)(620)로부터 제거된다. 워터마킹 명령, 암호화된 대칭 키(623) 및 객체의 허용된 이용을 규정하는 사용 조건(517) 같은 콘텐츠 제공자(들)(101)에 의해 제공된 권리 관리 정보가 또한 보유된다. --

이때, 상기 분해된 메타 데이터 SC(들)(620)는 오퍼 SC(들)(641)에 포함된다. 전자 디지털 콘텐츠 스토어(들)(103)는 또한 스토어 사용 조건(519)을 호출한 자체의 사용 조건을 첨부하거나, 또는 오퍼 SC(들)(641)로의 옵션을 구매한다. 이것은 디폴트의 세트를 통해 상호작용적으로 또는 자동적으로 구현될 수 있다. 상호작용적으로 처리되어 구성되면, 전자 디지털 콘텐츠 스토어(들)(103)는 콘텐츠 제공자(들)(101)에 의해 규정된 바와 같이 허용된 객체 사용 조건(517)의 세트로 프롬프트된다. 이때, 콘텐츠 제공자는 자신의 고객에게 제공하고자 하는 옵션(들)을 선택한다. 이들은 이제 새로운 사용 조건 또는 스토어 사용 조건(519)이 된다. 자동적으로 처리하기 위하여, 전자 디지털 콘텐츠 스토어(들)(103)는 모든 콘텐츠(113)에 제공될 디폴트 구매 옵션의 세트를 구성한다. 상기 디폴트 옵션은 콘텐츠 제공자(들)(101)에 의해 규정된 허용된 사용 조건(517)에 대비하여 자동적으로 검색되며, 어떠한 불일치도 없다면 오퍼 SC(들)(641)에 설정된다.

일단, 오퍼 SC(들)(641)가 생성되면, 오퍼 데이터베이스(181)에 저장되며, 메타 데이터 SC(들)(620)에 미리 할당된 저작물 ID로 인덱스된다. 상기 저작물 ID는, 이후 최종 사용자(들)로의 패키징 및 전송을 위해 오퍼 SC(들)(641)를 검색하고자 오퍼 데이터베이스(181)와 인터페이스할 때 고객에 의해 구매되고 있는 다운로드 가능한 콘텐츠(113)를 식별하기 위해 전자 디지털 콘텐츠 스토어(들)(103)에 의해 이용된다. 더 상세한 설명을 위하여 트랜잭션 처리기 모듈(175)을 살펴본다.

다른 실시예에서, 전자 디지털 콘텐츠 스토어(들)(103)는 그 사이트에서 콘텐츠 SC(들)(641)를 호스팅한다. 본 실시예는 콘텐츠 호스팅 사이트(들)(111)의 전자 디지털 콘텐츠 스토어(들)(103)로의 대체 같은 오퍼 SC(들)(641)로의 변경을 필요로 한다.

3. 트랜잭션 처리 모듈(175)

전자 디지털 콘텐츠 스토어(들)(103)는 클리어링하우스(들)(105)로의 빌링을 지시한다. 또한, 전자 디지털 콘텐츠 스토어(들)(103)는 클리어링하우스(들)(105)로부터 지시된 금융 클리어링을 요구할 수 있다. 다운로드 가능한 콘텐츠(113)에 대한 최종 사용자(들) 구매 요구를 처리하기 위한 2개의 기본 모드가 있다. 만약, 전자 디지털 콘텐츠 스토어(들)(103)가 구매의 금융 결제를 관리하고자 하지 않으며, 제품의 판매를 지배하는 어떠한 특별한 프로모션이나 인센티브도 없고, 구매 요구를 일괄 처리하기 위한 쇼핑 카트 메타포(metaphor)를 이용하지 않으면, 오퍼 SC(들)(641) 파일에 직접 콘텐츠(113) 다운로드 페이지상의 링크를 선택할 수 있다. 상기 오퍼 SC(들)(641)는 메타 데이터에 포함된 소매 가격 정보와 함께 구축되어 있어야 한다. 오퍼 SC(들)(641)에는 또한 판매 조건 및 기간을 갖는 구매 옵션을 나타내는 특별한 HTML 오퍼 페이지가 포함된다. 상기 페이지는 오퍼 SC(들)가 구축될 때 생성된 템플릿으로부터 구축된다. 최종 사용자가 오퍼 SC(들)(641)로의 직접 링크를 클릭하면, 오퍼 SC(들)(641)는 콘텐츠를 여는 헬퍼 애플리케이션을 착수시켜 브라우저 최종 사용자 장치(들)(109)로 다운로드되어, 오퍼 SC(들)(641)에 포함된 오퍼 페이지를 나타낸다. 상기 페이지는 신용 카드 정보 및 구매 옵션 선택을 포함한 고객 정보를 수집하기 위한 형태를 취한다. 이 형태는 금융 결제 및 처리를 위해 클리어링하우스(들)(105)에 직접 제공된다. 선택적으로, 상기 형태는 최종 사용자(들)의 신용 정보 또는 산업 표준 로컬 트랜잭션 관리기를 이용하기 위해 필요한 필드를 포함할 수 있다.

이제부터 전자 디지털 콘텐츠 스토어(들)(103)가 빌링을 관리하는 실시예를 설명한다. 구매 요구를 관리하는 더 일반적인 모드는 전자 디지털 콘텐츠 스토어(들)(103)가 금융 결제를 처리할 수 있도록 하고, 다운로드 인증을 최종 사용자(들)에게 제공한다. 이러한 방법은 전자 디지털 콘텐츠 스토어(들)(103)가 그 사이트에서 판매를 위해 제공된 다른 제품을 갖는 다운로드 가능한 콘텐츠(113)의 판매를 통합할 수 있도록 하고, 각 다운로드 요구에 대한 개별 과금 대신에 고객에게 하나만의 합쳐된 과금으로 구매 요구의 일괄 처리

를 허용하며, 전자 디지털 콘텐츠 스토어(들)(103)가 그 고객의 구매 패턴을 바로 추적하여 특별한 프로모션 및 클럽 옵션을 제공할 수 있도록 한다. 이러한 환경에서, 다운로드 가능한 콘텐츠(113)의 오퍼는 최종 사용자(들)에 의해 선택될 때 쇼핑 카트에 추가되며, 전자 디지털 콘텐츠 스토어(들)(103)의 현재 쇼핑 모델에서 수행되는 것과 같이 처리되고 금융적으로 결제된 쇼핑 페이지에 포함된다. 일단, 금융 결제가 완료되면, 이때 전자 디지털 콘텐츠 스토어(들)(100)의 상거래 관리 처리는 트랜잭션을 완료하기 위하여 트랜잭션 처리 모듈(175)을 호출한다.

트랜잭션 처리 모듈(175) 트랜잭션 처리 모듈(175)의 역할은 구매된 콘텐츠(113)의 다운로드를 개시 및 처리하기 위하여 최종 사용자 장치(들)(109)에 필요한 정보를 모으는 것이다. 이 정보는 구매 신청의 응답으로서 웹 서버에 의해 최종 사용자 장치(들)로 되전송되는 트랜잭션 SC(들)(640)로 패키징된다. 트랜잭션 처리 모듈(175)은 전자 디지털 콘텐츠 스토어(들)(103)의 상거래 관리 처리에서, 구매된 콘텐츠에 대한 저작물 ID, 트랜잭션 데이터(642) 및 구매 결제를 승인하는 CGI URL 또는 HTML의 3가지 정보를 필요로 한다.

저작물 ID는 방금 판매된 콘텐츠(113)와 연관된 메타 데이터 SC(들)(620)로 전자 디지털 콘텐츠 스토어(들)(103)에 제공된 값이다. 상기 저작물 ID는 오퍼 데이터베이스(181)로부터 연관된 오퍼 SC(들)(641)를 검색하기 위해 이용된다.

트랜잭션 데이터(642)는, 최종 사용자 장치(들)(109)에 다운로드된 콘텐츠(113)의 워터마크에 포함될 사용자 동일성 정보를 제공하기 위해서, 및 전자 디지털 콘텐츠 스토어(들)(103)에 의해 수행된 금융 결제 트랜잭션으로 처리하는 클리어링하우스(들)(105)를 상 관시킴을 위해 이후에 이용되는 전자 디지털 콘텐츠 스토어(들)(103)의 트랜잭션 처리 기능에 의해 제공된 정보의 구조이다. 클리어링하우스(들)(105)가 유효한 오더 SC(들)(650)를 수신하면, 판매된 콘텐츠(113)를 표시하는 트랜잭션을 로그하는데, 여기서 전자 디지털 콘텐츠 스토어(들)(103)는 콘텐츠 및 최종 사용자의 이름 및 트랜잭션 ID(535)를 포함한 이와 연관된 트랜잭션 데이터(642)를 판매한다. 트랜잭션 ID(535)는 금융 결제 트랜잭션으로의 참고를 제공한다. 이후, 상기 정보는 콘텐츠 제공자(들)(101)(또는, 그 에이전트)로부터 수신된 빌링 상태를 갖는 회계를 조정시 이용하기 위해 클리어링하우스(들)(105)에 의해 전자 디지털 콘텐츠 스토어(들)(103)로 복귀된다. 클리어링하우스 트랜잭션 로그(178)는 자신의 어떤 콘텐츠(113)가 판매되었는가를 판단하여 자신이 자신에게 소유된 로열티에 대하여 각 전자 디지털 콘텐츠 스토어(들)(103)에 빌을 작성할 수 있도록 하기 위하여 콘텐츠 제공자(들)(101)에 의해 이용될 수 있다. 이외에 빌링을 위한 다른 전자 수단이 콘텐츠 제공자(들)(101) 및 전자 디지털 콘텐츠 스토어(들)(103) 간의 회계 결제를 위하여 선택적으로 이용될 수 있다.

트랜잭션 SC(들)(640)에 제공된 정보 및 트랜잭션 SC(들)(640)의 보안 및 무결성은 구매 트랜잭션이 유효한 클리어링하우스(들)(105)에 충분한 신뢰성을 제공하기 때문에, 클리어링하우스(들)(105)에 의한 상기 판매의 로깅 전에 더 이상의 어떠한 검증도 필요없게 된다. 그러나, 전자 디지털 콘텐츠 스토어(103)는 그 회계에서 (상기 전자 디지털 콘텐츠 스토어(들)(103)가 상기 콘텐츠(113)의 판매를 위한 금전을 수집하였음을 콘텐츠 제공자(들)(101)에게 나타내서 클리어링하우스(들)(105)에 로그된 트랜잭션에)과금하기 전에 인증을 요구하기 위한 옵션을 갖을 수 있다. 인증/통지를 위한 상기 요구는 트랜잭션 데이터(642)에 플래그로 표시된다. 이러한 시나리오에서, 클리어링하우스(들)(105)는 전자 디지털 콘텐츠 스토어(들)(103)와 계약을 하여, 그 회계에서의 과금 전에 전자 디지털 콘텐츠 스토어(들)(103)로부터의 인증 및 암호화 키(623)의 릴리즈를 수신한다. 트랜잭션 ID(535)는, 전자 디지털 콘텐츠 스토어(들)(103)가 상기 요구를 최종 사용자와 함께 수행된 이전의 트랜잭션에 연관시킬 수 있도록 하는 상기 인증 요구의 부분으로 클리어링하우스(들)(105)로부터 전자 디지털 콘텐츠 스토어(들)(103)로 전달된다. 이 트랜잭션 ID(535)는 전자 디지털 콘텐츠 스토어(들)(103)가 이용하고자 하고, 오로지 그 이익만을 위한 소정의 단일 값일 수 있다.

트랜잭션 데이터(642)는 또한 고객 이름을 포함한다. 상기 이름은 구매를 할 때 사용자에게 의해 기입된 구매 형태의 사용자 이름 필드, 또는 전자 디지털 콘텐츠 스토어(들)(103)와의 소정의 유저 등록 처리중에 이미 등록된 정보로부터의 이름, 또는 상기 트랜잭션에서 이용된 카드와 연관된 신용 카드 정보로부터 얻어진 공식 이름일 수 있다. 이후, 상기 이름은 인가 워터마크(527)에 포함된다.

트랜잭션 데이터(642)는 또한 최종 사용자(들)에 의해 구매된 스토어 사용 조건(519)을 포함한다. 상기 정보는 인가 워터마크(527)에 포함되며, 카피 및 플레이 제어시 최종 사용자 장치(들)(109)에 의해 이용된다.

트랜잭션 처리 모듈(175)에 필요한 최종 파라미터는 구매 결제를 승인하는 CGI URL 또는 HTML 페이지이다. 이 목적은 전자 디지털 콘텐츠 스토어(들)(103)가 최종 사용자가 응답에 포함되기를 원하는 정보 모두와 금융 결제의 승인으로 최종 사용자(들)에게 응답할 수 있도록 하기 위한 것이다. 상기 HTML 페이지 또는 CGI URL은 트랜잭션 SC(들)(640)에 포함되며, 트랜잭션 SC(들)(640)가 수신되어 처리될 때 최종 사용자 장치(들)(109)의 브라우저 윈도우에 디스플레이된다.

트랜잭션 SC(들)(640)는 구매 신청을 처리한 후 전자 디지털 콘텐츠 스토어(들)(103)로부터 최종 사용자(들)로의 HTTP 응답이다. 직접적인 HTTP 응답으로 SC(들)을 전송하여 SC(들) 처리기 펌웨어 애플리케이션의 최종 사용자 장치(들)(109)상에 자동 로딩시켜서, 다른 최종 사용자(들) 개시 활동에 따르지 않고 트랜잭션의 자동 완료를 할 수 있다. 상기 처리는 이후에 최종 사용자 장치(들)(109) 및 플레이어 애플리케이션(195) 섹션에서 더 상세히 설명된다.

트랜잭션 처리 모듈(175)이 요구된 파라미터로 호출되면, 트랜잭션 데이터(642), 트랜잭션 승인 HTML 페이지 또는 참조 URL, SC(들)의 다른 필요한 보안 특징들을 포함한 트랜잭션 SC(들)(640)를 구축하고, 구매와 연관된 오퍼 SC(들)(641)를 검색하여 매입한다. 또한, 이후에 통지 인터페이스 모듈(176) 및 회계 조정 툴(179)에 의해 이용하기 위한 상기 트랜잭션에 관한 정보를 로그한다.

4. 통지 인터페이스 모듈(176)

통지 인터페이스 모듈(176)은 웹 서버측의 실행가능한 루틴(CGI 또는 NSAPI, ISAPI 등에 의해 호출가능한 기능)이다. 이것은 클리어링하우스(들)(105), 최종 사용자 장치(들)(109), 콘텐츠 호스팅 사이트(들)(111) 및 콘텐츠 제공자(들)(101)로부터의 선택적 요구 및 통지를 관리한다. 전자 디지털 콘텐츠 스토어(들)(103)가 통지를 선택적으로 요구할 수 있는 사건은 다음과 같다:

· 클리어링하우스(들)(105) 및 암호화 키(623)를 요구한 최종 사용자 장치(들)(109)가 지정된 콘텐츠(113)에 대한 암호화 키(623)를 릴리즈하고 있음을 클리어링하우스(들)(105)로부터 통지. 상기 통지는 최종 사용자 장치(들)(109)에 암호화 키(623)를 전송하기 전에 전자 디지털 콘텐츠 스토어(들)(103)로부터의 인증을 요구하기 위해 선택적으로 구성될 수 있다.

· 콘텐츠 SC(들)(630)가 최종 사용자 장치(들)(109)에 전송되었음을 콘텐츠 호스팅 사이트(들)(111)로부터 통지.

· 인가 SC(들)(630) 및 인가 SC(들)(660)가 수신되어 콘텐츠(113)를 처리하기 위해 성공적으로 이용되었거나 또는 훼손되었음을 최종 사용자 장치(들)(109)로부터 통지.

새로운 콘텐츠(113)가 현재의 프로모션 웹 사이트(156)에 배치되었음을 콘텐츠 제공자(들)(101)로부터 통지.

상기 통지들이 보안 디지털 콘텐츠 전자 배포 시스템 흐름(100)에 필수적인 단계는 아니지만, 전자 디지털 콘텐츠 스토어(들)(103)에게 판매 완료의 충족시 그 기록을 폐쇄할 수 있는 기회를 제공하기 위하여 옵션으로 제공된다. 이것은 또한 어떠한 기능이 나타나는가를 전자 디지털 콘텐츠 스토어(들)(103)가 알 수 있도록 함으로써 고객 서비스 요구를 관리하기 위해 필요한 정보를 제공하는데, 그 이유는 판매의 완료를 시도하는 중에 발행되는 에러 또는 트랜잭션의 금융 결제 때문이다. 또한, 상기 상태의 대부분은 필요에 따라 고객 서비스 인터페이스(184)를 통해 클리어링하우스(들)(105)로부터 얻어질 수 있다.

콘텐츠 프로모션 웹 사이트(156)에서 이용될 수 있는 새로운 콘텐츠(113)의 통지 빈도는 콘텐츠 제공자(들)(101)에 의해 결정된다. 통지는 각 새로운 메타 데이터 SC(들)(620)가 부가됨에 따라, 또는 날마다 모든 새로운 메타 데이터 SC(들)(620)가 부가됨에 따라 제공될 수 있다.

상기 통지 모두는 트랜잭션 로그(178)에서 이루어진 엔트리에 나타난다. 전자 디지털 콘텐츠 스토어(들)(103)가 자체적으로 상기 통지의 처리를 수행하고자 한다면, CGI 호출을 인터셉트할 수 있고, 그 유일한 기능을 구행하고, 이후 요구를 통지 인터페이스 모듈(176)에 선택적으로 전달한다.

5. 회계 조정 툴(179)

상기 회계 조정 툴(179)은 트랜잭션 로그(178)와 클리어링하우스(들)(105)의 로그를 비교하기 위해 클리어링하우스(들)(105)와 계약한다. 이것은 보안 디지털 콘텐츠 전자 배포 시스템(100)에 대한 회계에 관한 전자 디지털 콘텐츠 스토어(들)(103)에 도움을 주기 위해 이용될 수 있는 선택적 처리이다.

다른 실시예에서, 상기 툴은 콘텐츠 제공자(들) 및 클리어링하우스(들)(105)에 자동화된 주기적 지불을 위해 전자 화폐 전달을 제공하기 위해 갱신될 수 있다. 이것은 또한 트랜잭션 로그(178)에 대한 빌을 조정한 후 클리어링하우스(들)(105)로부터 전자 빌을 수신시 자동적으로 지불 처리를 하기 위해 디자인될 수 있다.

C. 방송 전자 디지털 콘텐츠 배포 서비스

방송은 주로 요구불 시청 및 청취를 개별화하기 위한 최종 사용자 장치(들)(109)와 전자 디지털 콘텐츠 스토어(들)(103) 사이에 개인 상호작용이 없는 일대 다수의 전송 방법을 말한다. 이것은 일반적으로 콘텐츠(113)가 미리 프로그램되는 디지털 위성 또는 케이블 기반 시설상에서 제공되어, 모든 최종 사용자 장치(들)(109)가 동일한 스트림을 수신할 수 있도록 한다.

하이브리드 모델은 또한 인터넷 접속을 통해 웹 배포 인터페이스 뿐만아니라 방송 서비스를 통한 고 대역폭 위성 또는 케이블 배포 인터페이스 모두를 공급할 수 있도록 하는 방식으로 조정된 디지털 콘텐츠 서비스를 사이트 디자인에 대량으로 제공하도록 규정될 수 있다. IRD 역채널 시리즈 인터페이스가 웹, 및 웹 항해를 지원하는 IRD와 접속된다면, 최종 사용자(들)는 구매를 위해 콘텐츠(113)를 미리보고 선택하는 역채널 인터넷 인터페이스를 통해 일반적인 방식으로 디지털 콘텐츠 서비스를 항해할 수 있다. 사용자는 고품질의 다운로드 가능한 콘텐츠(113)를 선택하고, 상기 선택을 구매하며, 인터넷 접속을 통해 필요한 인가 SC(들)(660) 모두를 수신할 수 있다. 웹 서비스는 방송 스케줄에 기초하여 상기 방식으로 다운로드하기 위하여 이용되거나, 또는 전체적으로 구매된 콘텐츠(113)에 기초하여 방송 스트림을 구축할 수 있음을 나타낼 수 있다. 이 방법은 웹 인터페이스를 통해 저 품질로 다운로드하기 위해 이용될 수 있는 전체 카탈로그 및 상기 방식으로 매일 이용될 수 있는 제한된 수의 특정한 콘텐츠(예컨대, 곡 또는 CDS)를 작성하는 적절한 장비를 구비한 유저에게 고품질의 콘텐츠(113)를 전달하기 위해 웹 기반의 디지털 콘텐츠 서비스를 방송 설비와 계약될 수 있도록 한다.

최종 사용자 장치(들)(109)와의 웹 인터페이스가 없는 다른 방송 모델이 디자인될 수 있다. 이 모델에서, 프로모션 콘텐츠는 최종 사용자 장치(들)(109)(즉, IRD)에 방송 전달을 위해 특별히 포맷된 디지털 스트림으로 패키징되며, 여기서는 스트림을 디코딩하기 위해서, 및 구매 선택이 이루어질 수 있는 프로모션형 콘텐츠를 최종 사용자에게 나타내기 위해 특별한 처리가 수행된다.

실제 구매 선택은 역채널 통신을 통해 최종 사용자 장치(들)(109)로부터 클리어링하우스(들)(105)로 개시될 수 있으며, 모든 데이터 교환을 수행하기 위하여 SC(들)를 이용할 수 있다. 전자 디지털 콘텐츠 스토어(들)(103)에 제공된 툴 세트는 대부분의 툴이 방송 위성 또는 케이블 오퍼링 뿐만아니라 포인트 투 포인트 인터넷 서비스 오퍼링 모두를 적용하는 방식으로 구성 및 개발되었다. SC(들)를 준비할 뿐만아니라 콘텐츠(113)를 취득 및 관리하기 위해 디지털 콘텐츠 웹 사이트 전자 디지털 콘텐츠 스토어(들)(103)에 의해 이용된 툴들은 또한 방송 기반 시설에 배포하기 위한 콘텐츠(113)를 관리하고 준비하기 위해 위성 기반의 전자 디지털 콘텐츠 스토어(들)(103)에 의해 이용된다. 웹 서비스상에서 배포된 SC(들)는 방송 서비스상에서 배포된 것과 같은 것이다.

X. 최종 사용자 장치(들)(109)

보안 디지털 콘텐츠 전자 배포 시스템(100)용 최종 사용자 장치(들)(109)에서의 애플리케이션은 2가지 주요 기능을 수행하는데, 첫 번째는 SC(들) 처리 및 카피 제어이고, 두 번째는 암호화된 콘텐츠(113)의 플레이백이다. 최종 사용자 장치(들)(109)가 퍼스널 컴퓨터 또는 특화된 전자 고객 장치이던 간에, 상기 기본 기능을 수행할 수 있어야 한다. 최종 사용자 장치(들)(109)는, 또한 플레이 리스트 생성, 디지털 콘텐츠 라이브러리, 콘텐츠 플레이백 중에 정보 및 이미지의 디스플레이, 및 외부 매체 장치로의 기록 같은 다양한 추가적인 특징 및 기능을 제공한다. 상기 기능은 상기 애플리케이션이 지원하는 서비스에 기초하여 변화하며, 장치의 타입마다 애플리케이션이 디자인된다.

A. 개요

이하, 도 10을 참조하면, 최종 사용자 장치(들)(109) 기능적 흐름, 주요 성분 및 처리가 도시된다. PC 기반 웹 인터넷 콘텐츠(113) 서비스를 지원하기 위해 선정된 애플리케이션은 SC(들) 처리기(192) 및 플레이어 애플리케이션(195)의 2개의 실행가능한 소프트웨어 애플리케이션으로 구성된다. SC(들) 처리기(192)는 SC(들) 파일/MIME 타입을 관리하기 위해 최종 사용자(들) 웹 브라우저(191)로의 헬퍼 애플리케이션으로 구성된 실행가능한 애플리케이션이다. 상기 애플리케이션은 전자 디지털 콘텐츠 스토어(들)(103), 클리어링하우스(들)(105) 및 콘텐츠 호스팅 사이트(들)(111)로부터 수신될 때마다 브라우저에 의해 착수된다. 이것은 SC(들)의 모든 필요한 처리를 수행하고, 최종적으로 최종 사용자(들)의 디지털 콘텐츠 라이브러리(196)에 콘텐츠(113)를 추가하는 역할을 한다.

플레이어 애플리케이션(195)은 최종 사용자(들)가 자신의 디지털 콘텐츠 라이브러리(196)에서의 콘텐츠(113)를 수행하기 위한 로드하고, 자신의 디지털 콘텐츠 라이브러리(196)를 관리하며, 허가되면 콘텐츠(113)의 카피를 생성하는 단독의 실행가능한 애플리케이션이다. 플레이어 애플리케이션(195) 및 SC(들) 처리기(192) 애플리케이션은 모두 자바, C/C++ 또는 소정의 동등한 소프트웨어로 기입될 수 있다. 양호한 실시예에서, 애플리케이션은 웹 사이트 같은 컴퓨터 판독가능 매체로부터 다운로드될 수 있다. 그러나, 다른 전달 메커니즘이, 또한 예컨대 컴퓨터 디스켓 또는 CDS 같은 컴퓨터 판독가능 매체상에 전달되는 것이 가능하다.

콘텐츠(113) 정보의 서칭 및 브라우징, 예컨대 곡 클립의 미리 보기 및 구매를 위한 곡의 선택은 모두 최종 사용자(들) 웹 브라우저(191)를 통해 관리된다. 전자 디지털 콘텐츠 스토어(들)(103)는 최근에 많은 콘텐츠(113) 소매 웹 사이트에 의해 제공되는 방식과 같이 쇼핑 경험을 제공한다. 최근의 웹 기반의 콘텐츠(113) 쇼핑에서의 최종 사용자(들)과의 차이는 이들이 이제는 그들의 쇼핑 카트에 추가될 다운로드 가능한 콘텐츠(113) 객체를 선택할 수 있는데 있다. 만약, 전자 디지털 콘텐츠 스토어(들)(103)가 다운로드 가능한 객체와 더불어 판매를 위해 이용가능한 다른 제품을 갖는다면, 최종 사용자(들)는 그의 쇼핑 카트에 물리적인 것과 전자적인 다운로드 가능한 제품의 조합한 것을 갖을 수 있다. 보안 디지털 콘텐츠 전자 배포 최종 사용자 장치(들)(109)는, 최종 사용자(들)가 체크 아웃한 후, 전자 디지털 콘텐츠 스토어(들)(103)에 자신의 최종 구매 인증을 신청할 때까지 수반되지 않는다. 이 시점 전에, 전자 디지털 콘텐츠 스토어(들)(103)용 웹 서버와 최종 사용자 장치(들)(109)상의 웹 브라우저(191) 사이에 모든 상호 작용이 이루어진다. 이것은 디지털 콘텐츠 클립의 미리 보기를 포함한다. 디지털 콘텐츠 클립은 SC(들)에 패키징되지 않고, 대신에 스트리밍 서버로부터 공급되거나 또는 다운로드 가능한 파일로서 전자 디지털 콘텐츠 스토어(들)의 웹 서버에 통합된다. 콘텐츠(113) 클립의 포맷은 시스템 구조에 의해 지시받지 않는다. 다른 실시예에서, 플레이어 애플리케이션(195)은 전자 디지털 콘텐츠 스토어(들)(103) 또는 클리어링하우스(들)(105)와 직접 상호작용하거나, 또는 프로모션 CD를 이용하여 오프라인과 상호작용할 수 있다.

B. 애플리케이션 설치

플레이어 애플리케이션(195) 및 헬퍼 애플리케이션(198)은 많은 웹 사이트로부터 다운로드를 위해 이용될 수 있는 자기 설치 실행가능한 프로그램으로 패키징된다. 클리어링하우스(들)(105)는 공용 웹 사이트에서 마스터 다운로드 페이지를 호스팅하는 중심 장소로서 작용한다. 이것은 설치 패키지가 다운로드될 수 있는 장소와의 링크를 포함한다. 설치 패키지는 다운로드 요구의 지형적 분산을 제공하기 위하여 콘텐츠 호스팅 사이트(들)(111)에서 이용될 수 있다. 각 참여 전자 디지털 콘텐츠 스토어(들)(103)는 또한 그들의 사이트로부터 다운로드를 위해 이용될 수 있는 패키지를 만들거나, 또는 클리어링하우스(들)(105)의 공용 웹 사이트에서 마스터 다운로드 페이지와의 링크를 제공할 수 있다.

다운로드 가능한 콘텐츠(113)를 구매하기 원하는 소정의 최종 사용자(들)은 상기 패키지를 다운로드하여 설치한다. 헬퍼 애플리케이션(198) 및 플레이어 애플리케이션(195) 모두를 언팩하여 설치하고, 또한 헬퍼 애플리케이션(198)을 설치된 웹 브라우저(들)에 구성한다.

설치의 일부로서, 공용/개인 키(661)는 오더 및 인가 SC(들)(660)를 처리시 이용하기 위해 최종 사용자 장치(들)(109)에 대하여 생성된다. 랜덤한 대칭 키(비밀 사용자 키)는 또한 인가 데이터베이스(197)에서의 곡 암호화 키를 보호시 이용하기 위하여 발생된다. 비밀 사용자 키(도시되지 않음)는 키를 다중 부분들로 분해하고, 최종 사용자(들)의 컴퓨터를 통해 다중 장소에 키의 피스들을 저장함으로써 보호된다. 코드의 상기 영역은 키가 어떻게 세그먼트되고, 어디에 저장되는 가를 누설하지 않도록 템퍼-레지스턴트(tamper-resistant) 소프트웨어 기술로 보호된다. 최종 사용자에 의한 상기 키로의 액세스를 방지하여 다른 컴퓨터와의 콘텐츠(113)의 공유 또는 해적 행위를 방지하는데 도움을 준다. 어떻게 상기 키가 이용되는 가에 대한 상세한 설명을 위해 SC(들) 처리기(192)를 참조한다.

템퍼-저항 소프트웨어 기술은 해커에 의한 컴퓨터 소프트웨어 애플리케이션으로의 비인증된 엔트리를 방지하기 위한 방법이다. 일반적으로, 해커는 사용 제한을 제거하기 위하여 소프트웨어를 이해하고 및/또는 변경하기를 원한다. 특히, 해킹될 수 없는 어떠한 프로그램도 존재하지 않는데, 이것이 템퍼-레지스턴스 소프트웨어가 "템퍼-프루프(tamper-proof)"로 불리지 않는 이유이다. 그러나, 템퍼-레지스턴스 보호 애플리케이션을 해킹하기 위한 많은 노력으로 인해 통상은 대부분의 해커를 단념케하는데, 그 이유는 그 노력이 이루어질 가능성이 없기 때문이다. 여기서의 노력은 아마도 CD상의 단일 곡 같은 콘텐츠(113)의 한 피스에 키를 액세스하여 얻을 수 있다.

템퍼 레지스턴트 소프트웨어 기술의 한 가지 타입은 IBM의 것이다. 이 코드가 도입된 한 가지 저작물은 IBM 싱크패드 770 랩탑 컴퓨터에 있다. 여기서, 템퍼-레지스턴트 소프트웨어는 컴퓨터에서 DVD 영화 플레이어를 보호하기 위하여 이용되었다. 디지털 영화의 출현 및 완전한 카피가 이루어지기 쉬움에 관심을 갖는 헐리우드 스튜디오 같은 디지털 콘텐츠 제공자(들)는 DVD 디스크(들)상의 영화가 카피 보호 메커니즘을 갖춰야 한다고 주장한다. IBM의 템퍼-레지스턴트 소프트웨어는 상기 카피 보호 메커니즘의 회피를 어렵게 한다. 이것은 템퍼-레지스턴트 소프트웨어에 대한 매우 일반적인 애플리케이션이며, 소프트웨어는 콘텐츠(113)의 소정의 보호된 타입의 사용에 규칙을 제공하기 위해 이용된다.

IBM의 템퍼-레지스턴트 소프트웨어는 침해자의 경로에 여러 타입의 장애물을 놓는다. 우선, 해커가 이용하는 오류 검출기 및 분해기 같은 표준 소프트웨어 툴의 효과를 좌절시키거나 또는 적어도 감소시키기 위한 기술을 포함한다. 다음으로, 자기 무결성 검사를 갖춰서, 단일 변화 또는 아주 소량의 변화도 검출되어 부정확한 동작을 일으키도록 한다. 마지막으로, 그 진정한 동작과 관하여 해커를 현혹시키기 위한 혼란제를 갖춘다. 후자의 기술이 특히 대중적이지만, 처음 두개의 기술은 암호화 및 디지털 기호 같은 암호문으로 공지된 툴들에 기초하여 구축된다.

C. 보안 컨테이너 처리기(192)

최종 사용자(들)가 거래를 위해 전자 디지털 콘텐츠 스토어(들)(103)에게 최종 구매 인증을 신청할 때, 이들은 자신의 쇼핑 카트에 수집하여, 자신의 웹 브라우저를 웹 서버로부터의 응답을 위해 대기하는 활성 상태로 남긴다. 전자 디지털 콘텐츠 스토어(들)(103)에서의 웹 서버는 구매를 처리하고, 금융 결제를 수행한 후, 트랜잭션 SC(들)(640)를 최종 사용자 장치(들)(109)로 복귀시킨다. SC(들) 처리기(192)(헬퍼 애플리케이션(198))은 트랜잭션 SC(들)(640)와 연관된 SC(들) 마임(mime) 타입을 처리하기 위해 웹 브라우저의 해 착수된다. 도 14는 본 발명에 따른 도 10에 도시된 바와 같이 로컬 라이브러리에 콘텐츠를 다운로드하는 플레이어 애플리케이션(195)의 사용자 인터페이스 스크린의 일례이다.

SC(들) 처리기(192)는 트랜잭션 SC(들)(640)를 열고, 그 안에 포함된 응답 HTML 페이지 및 오퍼 SC(들)(641)를 추출한다. 응답 HTML 페이지는 최종 사용자(들)의 구매를 승인하는 브라우저 윈도우에 디스플레이된다. 이때, 스텝 1401에서 오퍼 SC(들)(641)는 열리며, 예측된 다운로드 시간과 함께 콘텐츠(113)(예컨대, 곡 또는 앨범)명이 추출된다. 이때, 스텝 1402에서, 새로운 윈도우가 상기 정보로 디스플레이되며, 최종 사용자(들)는 콘텐츠(113)(예컨대, 음악에서 곡 또는 전체 앨범)의 다운로드(들)를 스케줄하기 위한 옵션을 제시받는다. 최종 사용자(들)는 바로 다운로드를 선택하거나, 또는 이후에 발생시키기 위한 다운로드를 스케줄할 수 있다. 이후의 시간이 선택되면, 다운로드 스케줄 정보는 로그에 세이브되며, 다운로드를 최종 사용자 장치(들)(109)가 상기 시간에 파워 온되면 스케줄된 시간에 개시된다. 컴퓨터가 스케줄된 다운로드 시간에 활성이 아니거나, 또는 통신 링크가 활성이 아니면, 최종 사용자(들)는 컴퓨터가 다음에 파워 업될 때 다운로드를 재스케줄하기 위해 프롬프트된다.

스케줄된 다운로드 시간이 발생할 때, 즉 바로 다운로드가 요구되었을 때, SC(들) 처리기(192)는 설치 시간에 발생한 최종 사용자(들)의 공용 키(661), 오퍼 SC(들)(641) 및 트랜잭션 SC(들)(640)에서의 정보로부터 오더 SC(들)(650)를 생성한다. 상기 오더 SC(들)(650)는 HTTP 요구를 통해 클리어링하우스(들)(105)로 전송된다. 클리어링하우스(들)(105)가 인가 SC(들)(660)로 복귀될 때, 헬퍼 애플리케이션(198)은 인가 SC(들)(660)를 처리하기 위해 다시 불러진다. 이때, 인가 SC(들)(660)는 열리며, 콘텐츠 호스팅 사이트(들)(111)의 URL은 참조된 오더 SC(들)(650)로부터 추출된다. 이후, 인가 SC(들)(660)는 콘텐츠 SC(들)(630)의 다운로드를 요구하는 브라우저에서 http를 통해 지정된 콘텐츠 호스팅 사이트(111)에 전송된다. 콘텐츠 SC(들)(630)가 브라우저로 돌아올 때, 헬퍼 애플리케이션(198)은 다시 불러진다. SC(들) 처리기(192)는 완료의 예측 시간 및 다운로드 진행 표시기와 함께 다운로드되고 있는 콘텐츠(113)의 이름을 디스플레이한다.

콘텐츠(113)가 SC(들) 처리기(192)에 의해 수신됨에 따라, 콘텐츠(113) 데이터를 해독화를 위해 메모리 버퍼에 로드시킨다. 버퍼의 크기는 암호화 알고리즘의 요건 및 워터마킹 기술(193)에 따라 달라지며, 해커 코드에 노출된 암호화되지 않은 콘텐츠(113)의 양을 감소시키기 위해 가능한 최소의 크기를 갖는다. 버퍼가 채워짐에 따라, 우선 자체적으로 개인 키를 이용하여 해독화된 인가 SC(들)(660)로부터 추출된 최종 사용자(들)의 키(623)(공용 키(661)에 대응함)를 이용하여 해독된다. 이후, 해독된 버퍼는 워터마킹 기능으로 전달된다.

워터마킹(193)은 인가 SC(들)(660)로부터 워터마킹 명령을 추출하고, 최종 사용자(들)의 개인 키를 이용하여 명령을 해독한다. 이후, 워터마킹 데이터는 상기 콘텐츠(113)가 구매한 전자 디지털 콘텐츠 스토어(들)(103)에 등록되거나, 또는 전자 디지털 콘텐츠 스토어(들)(103)가 등록 기능을 제공하지 않는다면, 신용 카드 등록 정보로부터 유도되는 구매자의 이름 같은 트랜잭션 데이터를 포함한 인가 SC(들)(660)로부터 추출된다. 워터마크에는 또한 상기 트랜잭션을 위해 로그된 특정 기록을 참조하기 위해 전자 디지털 콘텐츠 스토어(들)(103)에 의해 할당된 트랜잭션 ID(535) 및 구매 일자가 포함된다. 스토어 사용 조건(519)이 또한 플레이어 애플리케이션(195)의 카피 제어에 의해 이용되기 위하여 포함된다.

워터마킹(193)은 워터마킹 명령이 누설되지 않도록 템퍼 레지스턴트 코드 기술로 보호되기 때문에, 해커가 워터마크 기술 및 장소를 발견하는 것을 방지하게 된다. 이로서, 해커에 의한 워터마크의 제거 또는 변형을 방지할 수 있다.

상기 콘텐츠 버퍼에 소정의 필요한 워터마크를 적은 후, 버퍼는 재-암호화(194)를 위해 스캔블링 기능으로 전달된다. IBM의 SEAL 암호화 기술 같은 암호화 알고리즘을 효율적으로 보안하는 처리기는 랜덤한 대칭 키를 이용하여 콘텐츠(113)를 재-암호화하기 위해 이용된다. 일단 다운로드, 암호화 및 재암호화(194) 처리가 완료되면, 콘텐츠(113)를 최초로 암호화하기 위해 콘텐츠 제공자(들)(101)에 의해 이용된 암호화 키(623)는 무효화되고, 새로운 SEAL 키가 생성된 비밀 사용자 키를 이용하여 자체적으로 암호화되어 설치 시간에는 숨겨지게 된다. 이렇게 새로이 암호화된 SEAL 키는 인가 데이터베이스(107)에 저장된다.

다른 콘텐츠 제공자(들)(101)에서 수행된 소스 및 최종 사용자 장치(들)(109)에서 수행된 사용자 워터마킹이 효율화를 위한 산업 표

준으로 될 필요가 있다. 상기 표준은 아직도 발전하고 있다. 기술은 제어 정보가 음악에 매입되어 여러번 갱신되도록 이용될 수 있다. 카피 제어 표준 같은 시간이 더 안정될 때까지, 고객 장치에서의 권리 관리를 제공하기 위하여 카피 제어 워터마크에 의존하지 않도록, 다른 카피 제어 방법이 보안 디지털 콘텐츠 전자 배포 시스템(100)에 제공된다. 저장 및 플레이/기록 사용 조건 보안은 최종 사용자 장치(들)(109)와 연결되며 템퍼 레지스턴트 환경을 통해 보호되는 암호화된 DC 라이브러리 수집물(196)을 이용하여 실행된다. 소프트웨어 훅(hook)은 표준이 채택될 때 카피 제어 워터마킹을 지원하기 위한 위치에 있다. 최근에 AAC 및 다른 인코드된 오디오 스트림을 다양한 압축 레벨로 워터마킹하기 위한 지원이 있지만, 이 기술은 아직까지는 카피 제어 방법만으로 사용하기 위해 적용될 때는 다소 부족한 점이 있다.

해독 및 재-암호화(194) 처리는, 원 콘텐츠(113) 암호화 키, 새로운 SEAL 키, 비밀 사용자 키, 비밀 사용자 키가 어디에 저장되는가, 및 어떤 키가 세그먼트되는가를 누설하지 않도록 템퍼 레지스턴트 코드 기술로 보호되는 다른 코드의 영역이다.

해독화 및 재암호화(194)의 처리는 2가지 목적을 지원한다. SEAL 같은 알고리즘으로 암호화된 콘텐츠(113)를 저장하여 더 빠른 실시간 해독화를 가능하게 하며, DES 같은 많은 산업 표준 타입 알고리즘에서 필요한 것보다 해독화를 수행하기 위하여 훨씬 적은 처리기 활용을 필요로 한다. 이것은 디코드 및 플레이백 전에 콘텐츠(113)에 대한 전체 파일을 먼저 해독할 필요없이 콘텐츠(113)의 실시간 동시 해독-디코드-플레이백을 플레이어 애플리케이션(195)이 수행할 수 있도록 한다. SEAL 알고리즘 및 고효율 디코드 알고리즘은 동시 동작을 허용할 뿐만아니라 상기 처리가 훨씬 저전력 시스템 처리기에서 발생하도록 할 수 있다. 따라서, 상기 애플리케이션은 60MHz 펜티엄 시스템 정도의 낮은 한도 및 이보다 낮은 한도의 최종 사용자 장치(들)(109)상에 지원될 수 있다. 콘텐츠(113)가 최종적으로 저장된 암호화 포맷을 최초 암호화 포맷으로부터 분리하여, 최초 콘텐츠 암호화 알고리즘의 선택시 더 큰 유연성을 허용한다. 따라서, 광범위하게 채택되고 입증된 산업 표준 알고리즘이 보안 디지털 콘텐츠 전자 배포 시스템(100)의 더 향상된 디지털 콘텐츠 산업 채택을 위해 이용될 수 있다.

상기 해독 및 재암호화(194)의 두 번째 목적은, 상기 콘텐츠(113)를 암호화하기 위해 콘텐츠 제공자(들)(101)에 의해 이용된 원 마스터 키(623)가 상기 콘텐츠(113)를 인가한 최종 사용자 장치(들)(109)마다 저장되어야 하는 요건을 제거하기 위한 것이다. 인가 SC(들)(660)의 부분으로서 암호화된 마스터 키(623)는 아주 짧은 기간동안에 최종 사용자 장치(들)(109)의 하드디스크상에만 캐시되고, 아주 짧은 기간동안에 메모리에만 클리어로 있게 된다. 상기 실행 단계중에, 키(623)는 템퍼 레지스턴트 코드 기술을 통해 보호된다. 일단, 상기 해독 및 재암호화(194) 단계가 완료되면, 최종 사용자 장치(들)(109)상에 어떤 형태로도 상기 키(623)를 보유하지 않기 때문에, 해커로부터의 해적 행위의 확률을 크게 줄일 수 있다.

일단 곡이 재암호화되면, 디지털 콘텐츠 라이브러리(196)에 저장된다. 플레이어 애플리케이션(195)에 의한 이용을 위해 필요한 모든 메타 데이터는 스템 1403에서 연관된 오퍼 SC(들)(641)로부터 추출되어 디지털 콘텐츠 라이브러리(196)에 저장된다. 곡의 가사 같은 암호화된 메타 데이터의 소정 부분들은 다른 콘텐츠에서 상술된 것과 같은 방식으로 해독 및 재암호화된다. 콘텐츠(113)를 암호화하기 위해 이용된 동일한 SEAL 키가 암호화될 필요가 있는 소정의 연관된 메타 데이터에 이용된다.

D. 플레이어 애플리케이션(195)

1. 개요

보안 디지털 콘텐츠 전자 배포 플레이어 애플리케이션(195)(여기서는, 플레이어 애플리케이션(195)으로 칭함)은 CD, DVD 또는 다른 디지털 콘텐츠 플레이어 및 CD, DVD 또는 다른 디지털 콘텐츠 저장 관리 시스템 모두에 유사하다. 가장 간단한 예로, 곡 또는 비디오클립을 재생하는 것 같이 콘텐츠(113)를 수행하는 것이 있다. 다른 레벨에서, 자신의 디지털 콘텐츠 라이브러리(196)를 관리하기 위한 최종 사용자(들) 툴을 제공한다. 그리고, 곡(여기서는, 플레이-리스트로 칭함) 같은 콘텐츠 수집의 편집 및 수집을 위해서도 마찬가지로 중요하다.

플레이어 애플리케이션(195)은 콘텐츠 제공자(들)(101) 및 전자 디지털 콘텐츠 스토어(들)(103)의 요건에 독립적으로 선택되어 개별화될 수 있는 성분들의 수집으로 구성된다. 플레이어의 포괄적 버전이 설명되었지만, 개별화 또한 가능하다.

이하, 도 15를 참조하면, 도 10의 최종 사용자 장치(들)(109)에서 실행되는 플레이어 애플리케이션(195)의 처리 및 주요 성분들의 블록도가 도시된다.

플레이어 객체 관리자(1501)의 보조 시스템을 구성하는 여러 개의 성분 세트가 있다: 1. 최종 사용자 인터페이스 성분(1509)

2. 카피/플레이 관리 성분(1504)

3. 해독(1505), 압축 해제(1506), 플레이백 성분(1507), 및 기록을 포함할 수 있음

4. 데이터 관리(1502) 및 라이브러리 액세스 성분(1503)

5. 애플리케이션간 통신 성분(1508)

6. 다른 갖가지 (설치 등의) 성분

상기 각 세트들에서 이로부터의 성분이 다음의 요건에 기초하여 선택될 수 있다: • 플랫폼(윈도우, 유닉스 등) • 통신 프로토콜(네트워크, 케이블 등) • 콘텐츠 제공자(들)(101) 또는 전자 디지털 콘텐츠 스토어(들)(103) • 하드웨어(CD, DVD 등) • 클리어링하우스(들)(105) 기술 등이하의 섹션들은 여러 가지 성분 세트를 상세히 설명한다. 마지막 섹션은 상기 성분들이 포괄적 플레이어에 어떻게 구

성되는가를 상세히 설명하고, 성분들이 어떻게 개별화되는 가를 설명하다.

다른 실시예에서, 플레이어 애플리케이션(195) 및 SC(들) 처리기(192)의 성분이 프로그래머의 소프트웨어 툴 키트의 일부로 이용될 수 있다. 상기 툴 키트는 상기 리스트된 포괄적 플레이어 애플리케이션의 성분과의 규정된 인터페이스를 제공한다. 상기 규정된 인터페이스는 API, 즉 애플리케이션 프로그래밍 인터페이스의 형태로 있다. 상기 API를 이용하는 개발자는 고레벨 애플리케이션 프로그램으로부터 성분의 소정의 기능을 실행할 수 있다. API를 상기 성분들에 제공함으로써, 프로그래머는 소정의 상기 성분들의 자원 및 상기 기능들을 재생성할 필요없이 개별화된 플레이어 애플리케이션(195)을 신속히 개발할 수 있다.

2. 최종 사용자 인터페이스 성분(1509)

상기 세트로부터의 성분은 플레이어 애플리케이션(195)의 온-스크린 표시를 제공하기 위하여 결합된다. 디자인이 상기 성분의 어떠한 한정적 레이아웃 없이 구축될 수 있음을 유념한다. 이러한 한 가지 레이아웃이 포괄적 플레이어에 제공된다. 콘텐츠 제공자(들)(101) 및/또는 전자 디지털 콘텐츠 스토어(들) 및 다른 요건들로부터의 요건에 기초하여, 다른 레이아웃이 가능하다.

상기 세트는 최종 사용자 디스플레이(1510)를 나타내기 위해 이용되는 성분으로 개시하는 보조 그룹들로 그룹화되고, 메타 데이터의 표시 및 오디오 플레이백 같은 저레벨 기능에서 이용되는 최종 사용자 제어(1511)로 볼리우는 제어를 관리한다. 다음에, 최종 사용자 디스플레이 성분(1510)은 특별한 기능 그룹핑(플레이-리스트, 디지털 콘텐츠 라이브러리)으로 더 분할되며, 이때 객체 컨테이너 성분은 상기 저레벨 성분의 그룹핑 및 배치를 위해 이용된다.

이하에 리스트한 성분들 내에서, CD 또는 다른 기록가능한 매체로의 콘텐츠(113)의 카피 또는 CDS를 생성하기 위한 소정의 참조는 플레이어 애플리케이션(195)이 상기 기능을 제공받은 경우에만 적용된다. 상기 구문에서의 용어 "CD"는 포괄적인 것으로서, 또한 미니디스크 또는 DVD 같은 여러 가지 다른 외부 기록 장치를 표시할 수 있다.

도 16은 본 발명에 따른 도 15의 플레이어 애플리케이션(195)의 일례인 사용자 인터페이스 스크린이다. 최종 사용자 제어(1511)의 기능은 다음의 것들을 포함한다(최종 사용자 인터페이스의 대응하는 스크린은 1601-1605로 도시된다):

콘텐츠(113)를 수행하기 위한 제어: • 플레이/정지 버튼 • 플레이 버튼 • 정지 버튼 • 일시 정지 버튼 • 앞으로 스킵 버튼 • 뒤로 스킵 버튼 • 볼륨 제어 • 트랙 위치 제어/디스플레이 • 오디오 채널 볼륨 레벨 디스플레이 등.

콘텐츠(113)와 연관된 메타 데이터를 디스플레이하기 위한 제어 • 표지 그림 버튼 • 표지 그림 객체 • 가수 사진 버튼 • 가수 사진 객체 • 트랙 리스트 버튼 • 트랙 리스트 정보 객체 • 트랙 리스트 선택기 객체(플레이하기 위해 클릭함) • 트랙명 객체 • 트랙 정보 객체 • 트랙 가사 버튼 • 트랙 가사 객체 • 트랙 가수명 객체 • 트랙 신용 버튼 • 트랙 신용 객체 • CD명 객체 • CD 신용 버튼 • CD 신용 객체 • 포괄(구성가능한) 메타 데이터 버튼 • 포괄 메타 데이터 객체 등.

최종 사용자 디스플레이(1510)에 대한 기능은 다음의 것들을 포함한다(최종 사용자 인터페이스의 대응하는 스크린은 1601-1605에 도시된다): 디스플레이 컨테이너의 플레이-리스트 • 플레이-리스트 관리 버튼 • 플레이-리스트 관리 윈도우 • 디지털 콘텐츠 서치 버튼 • 디지털 콘텐츠 서치 규정 객체 • 디지털 콘텐츠 서치 신청 버튼 • 디지털 콘텐츠 서치 결과 객체 • 선택된 서치 결과 아이템을 플레이-리스트로 카피 버튼 • 플레이-리스트 객체(편집가능함) • 플레이-리스트 세이브 버튼 • 플레이-리스트 플레이 버튼 • 플레이-리스트 일시 정지 버튼 • 플레이-리스트 재시작 버튼 • 플레이-리스트로부터 CD 생성 버튼 등.

• 디지털 콘텐츠 라이브러리(196)의 디스플레이 • 디지털 콘텐츠 라이브러리 버튼 • 디지털 콘텐츠 라이브러리 윈도우 • 디지털 콘텐츠 캐터고리 버튼 • 디지털 코너콘텐츠 캐터고리 객체 • 가수축 버튼 • 장르축 버튼 • 레이블축 버튼 • 캐터고리축 버튼 • 삭제 버튼 • 부가에서 재생 리스트로의 버튼 • CD로의 카피 버튼 • 곡 리스트 객체 • 곡 리스트 디스플레이 컨테이너 등컨테이너 및 기타 • 플레이어 윈도우 컨테이너 • 오디오 제어 컨테이너 • 메타 데이터 제어 컨테이너 • 메타 데이터 디스플레이 컨테이너 • 툴바 컨테이너 객체 • 샘플 버튼 • 다운로드 버튼 • 구매 버튼 • 녹음 버튼 • 플레이어명 객체 • 레이블/제공자/스토어 광고 객체 • 레이블/제공자/스토어 URL 버튼 • 가수 URL 버튼 등3. 카피/플레이 관리 성분(1504)

상기 성분은 암호화 키의 셋업, 워터마크 처리, 카피 관리 등을 처리한다. 인터페이스는 또한 클리어링하우스(들)(105)와의 통신, 구매 요구의 전송, 및 페이-퍼-리슨, 즉 콘텐츠로의 각 액세스가 산출되는 경우 같은 특별한 서비스를 위해 존재한다. 현재, 클리어링하우스(들)(105)와의 통신은 SC(들) 처리기(192)에 의해 처리된다.

최종 사용자 장치(들)(109)를 통한 플레이어 애플리케이션(195)의 이용은 인가 데이터베이스(197) 같은 데이터베이스로 로그된다. 플레이어 애플리케이션(195)에 의한 콘텐츠의 각 이용의 추적은 클리어링하우스(들)(105) 또는 콘텐츠 제공자(들)(101) 또는 전자 디지털 콘텐츠 스토어(들)(103) 또는 전송 기반 시설(107)에 지시되어 결합된 소정의 사이트에 전송될 수 있다. 이러한 전송은 사용 정보를 로그 사이트에 업로드시키기 위해 예정된 시간에 스케줄될 수 있다. 일례로 미리 결정된 예정 시간은 전송 기반 시설(107)이 네트워크 트래픽으로 혼잡하지 않는 오전 일찍이다. 공지된 기술을 이용하는 플레이어 애플리케이션(195)은 스케줄된 시간에 동작하여 정보를 코덱 로그 데이터베이스로부터 로그 사이트에 전송한다. 로그 사이트 정보를 검토함으로써, 콘텐츠 제공자(들)(101)는 그들의 콘텐츠(113)의 인기를 측정할 수 있다.

다른 실시예에서, 로그 사이트로의 이후의 업로딩을 위해 콘텐츠(113)의 사용을 로그하는 대신에, 콘텐츠(113)의 이용이 콘텐츠(113)의 이용시마다 로그 사이트로 갱신된다. 예를 들어, 최종 사용자 장치(들)(109)에 저장된 콘텐츠(113)를 DVD 디스크, 디지털 테이프, 플래시 메모리, 미니 디스크 또는 동등한 판독/기입가능한 이동성 매체 같은 외부 장치에 복사 또는 카피할 때, 사용이 로그 사이트에 갱신된다. 이것은 콘텐츠(113)가 구매될 때 전송된 사용 조건(206)으로 콘텐츠(113)를 카피하기 위한 전제 조건일 수 있다. 이것은 콘텐츠 제공자(들)(101)가 콘텐츠(113)상에 자신의 플레이, 복사 또는 다른 활동을 하는 동안 그들의 콘텐츠(113)의 사용을

정확하게 추적할 수 있도록 한다.

또한, 콘텐츠(113)에 관한 다른 정보가 로그 사이트에 갱신될 수 있다. 예를 들어, 콘텐츠(113)가 수행되었던 최근 시간(예컨대, 시간 및 일자), 얼마나 많이 콘텐츠(113)가 수행되었는가, 콘텐츠(113)가 DVD 디스크, 디지털 테이프 또는 미니 디스크 같은 인증된 외부 장치에 복사 또는 카피되었는가의 정보일 수 있다. 가족의 다른 구성원 같이 최종 사용자 장치(들)(109)상의 단일 플레이어 애플리케이션(195)에 다수의 다른 사용자가 있는 경우, 콘텐츠(113) 사용자의 식별은 사용 정보와 함께 로그 사이트에 전송된다. 로그 사이트에 갱신된 사용 조건을 검토함으로써, 콘텐츠 제공자(들)(101)는 실제 사용, 사용자의 식별 및 콘텐츠(113)가 수행된 횟수에 기초하여 콘텐츠(113)의 인기를 측정한다. 실제 사용 측정은 텔레비전에 대한 닐슨 시청률 구조 또는 전화 측정 같은 샘플링 방법을 이용하여 상기 시스템이 시스템상에서 더 실제적으로 구동되도록 하며, 여기서는 제한된 수의 사용자만이 어떤 한 시점에서 예측된 결과로서 샘플된다. 본 실시예에서, 실제 사용은 전자 디지털 콘텐츠 스토어(들)(103) 또는 콘텐츠 제공자(들)(101) 같은 지정된 웹 사이트상으로 로그 백시켜 사용자에게 대한 측정을 할 수 있다.

4. 해독(1505), 압축 해제(1506) 및 플레이백 성분(1506)

상기 성분은 데이터 관리 및 라이브러리 액세스 성분으로부터 얻어진 오디오 데이터를 로크 해제하기 위하여 카피/플레이 관리 성분 에 의해 얻어진 키를 이용하고, 이것의 플레이백을 준비하기 위하여 적절한 압축 해제를 적용하며, 이것을 플레이하기 위하여 시스템 오디오 서비스를 이용한다. 다른 실시예에서, 메타 데이터 및 라이브러리 액세스 성분으로부터 얻어진 오디오 데이터는 CDS, 디스켓, 테이프 또는 미니 디스크 같은 이동성 매체에 카피될 수 있다.

5. 데이터 관리(1502) 및 라이브러리 액세스 성분(1503)

상기 성분들은 최종 사용자(들)의 시스템상의 여러 가지 저장 장치상에서의 곡 데이터를 저장 및 검색할 뿐만아니라 저장된 곡들에 관한 정보의 요구를 처리하기 위해 이용된다.

6. 애플리케이션간 통신 성분(1508)

상기 성분들은, 플레이어 애플리케이션(195)을 불러올 수 있는 보안 디지털 콘텐츠 전자 배포 플레이어와 다른 애플리케이션(예컨대, 브라우저, 헬퍼-애플리케이션 및/또는 플러그-인) 간의 조화를 위해 이용되며, 상기 플레이어 애플리케이션(195)은 이러한 기능을 수행할 때 이용하기 위해 필요하다. 예를 들어, URL 제어가 취해지면, 적절한 브라우저를 불러와서 이것을 적절한 페이지에 로드 시키도록 명령한다.

7. 다른 기타 성분들

상기 카테고리(예컨대, 설치)에 포함되지 않는 개별 성분은 여기서 그룹화된다.

8. 포괄적 플레이어

본 섹션에서, 플레이어 애플리케이션(195)의 버전으로의 상기 성분들의 결합이 설명된다. 이것은, 플레이어 애플리케이션(195)이 소프트웨어 객체에 기초하여 개별화를 위해 디자인되기 때문에, 가능한 많은 다른 예들중 하나이다.

플레이어 객체 관리자(1501)는 모든 다른 성분들을 출당하는 소프트웨어 프레임워크이다. 상기 섹션에서 설명된 바와 같이, 상기 도면에서의 플레이어 객체 관리자(1501) 아래의 블록은 소정의 플레이어를 필요로 하지만, 이용되는 암호화 또는 스크램블링의 형태와 같은 것, 오디오 압축 타입, 콘텐츠(113) 라이브러리에 대한 액세스 방법 등에 따라 달라지는 특화된 버전으로 대체될 수도 있다.

상기 플레이어 객체 관리자(1501)는 주로 플레이 또는 서치되고 있는 콘텐츠(113)와 연관된 메타 데이터로부터 유도되는 가변 객체(1512)이다. 상기 가변 객체는 최종 사용자 제어(1511)로부터 수신된 입력 및 최종 사용자 디스플레이(1510)를 통해 최종 사용자 장치(들)(109)에 이용될 수 있다. 모든 객체가 구성가능하며, 모든 콘텐츠의 레이아웃이 개별화가능하다. 상기 객체는 C/C++, 자바 또는 소정의 동등한 프로그래밍 언어로 실행될 수 있다.

플레이어 애플리케이션(195) 이용다음의 실시예는, 최종 사용자 장치(들)(109)상에서 실행되는 플레이어 애플리케이션(195)이 콘텐츠(113)가 음악인 오디오 플레이어인 예에 대한 것이다. 다른 타입의 콘텐츠(113)가 플레이어 애플리케이션(195)에 의해 지원될 수 있음을 당 기술에 숙련된 지식을 가진 자들은 이해할 수 있을 것이다. 일반적인 오디오 애호가는 곡을 보유한 CDS의 라이브러리를 갖게 된다. 이들 모두는 보안 디지털 콘텐츠 전자 배포 시스템(100)에서 이용될 수 있다. 전자 디지털 콘텐츠 스토어(들)(103)로부터 구매한 곡들의 세트는 자신의 시스템상의 디지털 콘텐츠 라이브러리(196)에 저장된다. 물리적 CDS와 유사한 곡의 그룹핑은 플레이-리스트로서 저장된다. 일부 경우, 플레이 리스트는 정확히 CD를 에뮬레이트한다(예컨대, 상용가능한 CD의 모든 트랙들이 전자 디지털 콘텐츠 스토어(들)(103)로부터 CD의 온라인 버전으로 구매되고, CD와 동일한 플레이-리스트로 규정됨). 그러나, 대부분의 플레이-리스트는 이들이 자체의 시스템상의 디지털 콘텐츠 라이브러리에 저장된 곡을 그룹화하기 위해 최종 사용자(들)에 의해 구성된다. 그러나, 설명의 확실화를 위하여, 음악 CD로 이루어진 주문의 예는 용어 "플레이-리스트"가 언급될 때 이용된다.

최종 사용자(들)가 플레이어 애플리케이션(195)을 시작할 때, SC(들) 처리기(192) 애플리케이션으로부터 불러오기를 통해 시작하는 것보다는, 액세스된 최근의 플레이-리스트로 미리 로드시키는 것이 좋다. 만약, 디지털 콘텐츠 라이브러리(196)에 어떠한 플레이-리스트도 없다면, (사용자가 프레퍼런스 설정을 통해 상기 특징을 턴 오프하지 않는다면)플레이-리스트 편집기는 자동적으로 시작된다. 더 상세한 설명을 아래의 플레이-리스트를 참조한다.

또한, 바로 곡-플레이 모드로 진입한 경우에, 인수에 따라 특정한 곡을 갖는 플레이어 애플리케이션(195)이 불러와질 수 있다. 선택적으로, 곡은 플레이하기 위한 준비를 할 수 있지만, 처리 전에 최종 사용자(들)에 의해 활동 대기할 수도 있다. 상기 상황에 대한 더 상세한 것은 이하의 곡 플레이를 참조한다.

플레이-리스트(최종 사용자 인터페이스(1603)의 스크린에 대응함)최종 사용자(들)가 플레이-리스트 기능을 불러올 때, 다음과 같은 이용가능한 기능들이 있다: • 플레이-리스트 열기 • 다이제스트 콘텐츠 라이브러리언이 선택을 위해 저장된 플레이-리스트들중 한 리스트를 디스플레이하기 위해 불러와짐. 또한, 더 상세한 정보에 대해서는 이하의 디지털 콘텐츠 라이브러리언을 참조한다.

• 플레이-리스트 편집 • 플레이-리스트가 이미 로드되었다면 현재의 플레이-리스트로 준비된 플레이-리스트 편집기(하기 참조)를 불러옴. 만약, 그렇지 않다면, 편집기는 시작을 위하여 빈 플레이-리스트를 생성한다.

• 플레이-리스트 실행 • 곡들이 선택된 곡으로(또는, 어떠한 곡도 선택되지 않는다면, 플레이-리스트의 처음으로) 시작하는 시간에 하나가 플레이됨. 플레이-리스트 편집기에서 설정된 옵션은 플레이백의 시퀀싱에 영향을 미친다. 그러나, 여기서는 플레이-리스트의 상기 플레이에 대한 상기 옵션을 무시하기 위해 이용될 수 있는 제어가 있다.

• 곡 플레이 • 플레이-리스트로부터 선택된 곡만이 플레이됨. 더 이상의 정보는 이하의 곡 플레이를 참조한다.

• 플레이-리스트 정보 • 플레이-리스트에 관한 정보를 디스플레이 • 곡 정보 • 플레이-리스트 내에서 선택된 곡에 관한 정보를 디스플레이함 • 웹 사이트 방문 • 상기 플레이-리스트와 연관된 웹 사이트를 브라우저에 로드시킴 • 라이브러리언 • 디지털 콘텐츠 라이브러리언 윈도우 열기. 또한, 더 이상의 정보에 대해서는 이하의 디지털 콘텐츠 라이브러리언을 참조함.

플레이-리스트 편집기(최종 사용자 인터페이스(1603)의 스크린에 대응함):플레이-리스트 편집기를 불러올 때, 최종 사용자(들)의 옵션이 있다: • 플레이-리스트 보기/로드/삭제 • 디지털 콘텐츠 라이브러리언은 로드 또는 삭제를 위한 것의 선택을 위해 저장된 플레이-리스트들중 한 리스트를 디스플레이하기 위해 불러와짐. 또한, 더 이상의 정보는 이하의 디지털 콘텐츠 라이브러리언을 참조함.

• 플레이-리스트 세이브 • 플레이-리스트의 현재 버전이 디지털 콘텐츠 라이브러리(196)에 세이브됨.

• 곡 삭제 • 현재 선택된 곡은 플레이-리스트로부터 삭제됨.

• 곡 추가 • 디지털 콘텐츠 라이브러리언이 플레이-리스트에 추가하기 위한 곡의 선택을 위해 곡-서치 모드에서 불러와짐.

• 곡 정보 설정 • 플레이-리스트 내에서 선택된 곡에 관한 정보 변화 허용 및 디스플레이. 상기 정보는 플레이-리스트 내에 저장되며, 디지털 콘텐츠 라이브러리(196) 내에 저장된 곡에 관한 정보를 변경시키지 않음.

• 디스플레이된 곡 타이틀 • 곡에 관한 최종 사용자(들) 메모 • 곡을 플레이시 도입 지연 • 곡을 플레이한 후 후속 지연 • 플레이할 때 곡에서의 시작-포인트 • 플레이할 때 곡에서의 종료-포인트 • 랜덤한 모드에 대한 웨이팅(Weighting) • 상기 곡 등에 대한 볼륨 조정 • 플레이-리스트 속성을 설정: 상기 플레이-리스트의 속성 변화 허용 및 디스플레이. 상기 속성들은 다음과 같이 설정될 수 있다:

• 플레이-리스트 타이틀 • 플레이-리스트 모드(랜덤, 순차적, 등) • 반복 모드(한번 플레이, 끝날 때마다 재시작, 등) • 상기 플레이-리스트에 관한 최종 사용자(들) 메모라이브러리언(최종 사용자 인터페이스(1601)의 스크린에 대응함): • 디지털 콘텐츠 라이브러리언 윈도우 열기. 또한, 더 이상의 정보에 대해서는 이하의 디지털 콘텐츠 라이브러리언을 참조함.

곡 플레이인수에 따라 곡을 갖는 플레이어 애플리케이션(195)을 불러오거나, 또는 플레이-리스트로부터 또는 디지털 콘텐츠 라이브러리언 내에서 플레이를 위한 곡을 선택함으로써, 곡이 플레이를 위한 준비가 되었을 때, 다음과 같은 최종 사용자(들)의 옵션들이 있다:(최종 사용자 인터페이스(1601)의 스크린에 대응함): • 플레이 • 일시 정지 • 정지 • 뒤로 스킵 • 앞으로 스킵 • 볼륨 조정 • 트랙 위치 조정 • 가사 보기 • 신용 보기 • CD 표지 보기 • 가수 사진 보기 • 트랙 정보 보기 • 다른 메타 데이터 보기 • 웹 사이트 방문 • 플레이-리스트 • 라이브러리언 등디지털 콘텐츠 라이브러리언 디지털 콘텐츠 라이브러리언은 곡 또는 플레이-리스트를 선택하고 있을 때, 조용히 불러와지거나, 또는 최종 사용자(들)의 시스템에서의 곡 라이브러리의 관리를 위해 자체의 윈도우에서 열릴 수 있다. 이 경우, 다음과 같은 최종 사용자(들)의 옵션들이 있다:

곡에서의 작업:모두를 가수, 카테고리, 레이블 등으로 분류시킴곡들을 가수, 카테고리, 레이블 등으로 선택함선택된 곡들을 현재의 플레이-리스트에 추가시킴(가능하다면)곡을 CD에 카피시킴곡을 삭제함곡을 카테고리 등에 추가시킴플레이-리스트에서의 작업:이름으로 분류시킴카테고리로 분류시킴키워드로 서치함포함된 곡 타이틀로 서치함선택된 플레이-리스트를 로드시킴플레이-리스트를 개명함플레이-리스트를 삭제함(가능하다면)선택된 플레이-리스트 등으로부터 CD를 생성이하, 본 발명에 따라 독립적으로 콘텐츠를 추적하기 위한 최종 사용자 장치(9)상에서 실행하기 위한 처리의 흐름도인 도 18을 참조한다. 콘텐츠 ID(1802)는 콘텐츠 준비중에 콘텐츠 제공자(101)에 의해 제공된다. 일 실시예에서, 콘텐츠 ID(1802)는 보안 콘텐츠인 패커 툴(152)로 콘텐츠 생성 처리를 하는동안의 콘텐츠 SC(들)(630)의 일부이다. 다른 실시예에서, 콘텐츠 ID(1802)는 처리되고 있는 콘텐츠에 유일한 식별자이다.

트랜잭션 ID(535)는 이미 설명된 바와 같이 트랜잭션 처리기 모듈(175)에 의해 구축된 트랜잭션 SC(들)(640)에서의, 콘텐츠 ID(1802)와 함께 트랙잭션 데이터(642)의 일부이다. 트랜잭션 ID(535)는 최종 사용자 장치(들)(109)로부터의 모든 구매 트랜잭션상에서의 각각에 대한 유일 식별자이다. 또한, 아이템 번호(1806)는 각 피스마다의 전자 디지털 콘텐츠 스토어(103)에 의해 발생된 유일 식별자 또는 트랜잭션의 일부를 형성하는 멤버 또는 타이틀이다.

이하, 최종 사용자 장치(109)에 의해 수신되는 최종 사용자 장치(109)상에서의 동작에 초점을 맞춘다. 또한, 트랜잭션 ID(535)에 포함된 콘텐츠 ID(1802)를 갖는 오퍼 SC(들)이 수신된다. 구매 ID(1812)는 최종 사용자 장치(109)상에서 생성된다. 일 실시예에서, 구매 ID는 3개의 번호들, 특히 콘텐츠 ID(1802), 트랜잭션 ID(1802), 아이템 번호(1806)의 연결 동작(1810)이다. 연결 동작(1810) 이외의 다른 타입의 조합이, 예컨대 3개의 번호들 모두를 함께 해싱하거나 또는 유일 구매 ID(1812)에서 나타나는 다른 수학적 조합 같은 구매 ID(1812)를 발생하기 위하여 이용될 수 있다. 3개의 번호를 결합하는 처리는 구매 ID 계산으로의 비인증된 액세스를 방지하기 위하여 플레이어 애플리케이션에서 이미 상술된 템퍼 레지스턴트 코드를 이용하여 이루어질 수 있다.

일단, 유일 구매 ID(1812)가 콘텐츠(113)의 각 피스마다 생성되거나 연관되면, 최종 사용자 장치(109)상에서의 플레이어 애플리케이션(195)은, 최종 사용자 장치(109)상에 저장된 꼭 같은 동일한 콘텐츠(113)의 하나 이상이 카피가 있더라도, 콘텐츠(113)의 각 피스마다 스토어 사용 조건(519)을 트랙할 수 있다.

발명의 효과

본 발명의 특정한 실시예가 설명되었지만, 본 발명의 사상 및 범주를 이탈하지 않는 범위 내에서 상기 특정한 실시예의 변화가 이루어질 수 있음을 당 기술에 숙련된 지식을 가진 자들은 이해할 수 있을 것이다. 따라서, 본 발명의 범주는 특정한 실시예에 한정되지 않으며, 첨부된 청구항들은 본 발명의 범주 내에서 일부 및 모든 응용, 변형 및 실시예들을 수용하도록 의도된다.

(57)청구의 범위

청구항1

디지털 콘텐츠 플레이어상의 디지털 콘텐츠를 유일하게 식별하기 위한 방법에 있어서,
콘텐츠 제공자로부터 수신된 콘텐츠를 유일하게 식별하는 제 1 식별자를 수신하는 단계와,
상기 콘텐츠가 수신되는 트랜잭션을 유일하게 식별하는 제 2 식별자를 수신하는 단계와,
상기 콘텐츠가 수신되는 트랜잭션에서의 아이템을 유일하게 식별하는 제 3 식별자를 수신하는 단계, 및
상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자의 수학적 조합에 기초하여 제 4 유일 식별자를 생성하는 단계를 포함하는 디지털 콘텐츠 식별 방법.

청구항2

제 1 항에 있어서, 상기 생성 단계는,
상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자의 연결(concatenation)에 기초하여 제 4 유일 식별자를 생성하는 단계를 포함하는 디지털 콘텐츠 식별 방법.

청구항3

제 1 항에 있어서, 상기 제 2 식별자 수신 단계는,
상기 콘텐츠를 판매하는 스토어로부터 유일 식별자를 수신하는 단계를 포함하는 디지털 콘텐츠 식별 방법.

청구항4

제 3 항에 있어서, 상기 제 3 식별자 수신 단계는,
상기 콘텐츠를 판매하는 스토어로부터 유일 식별자를 수신하는 단계를 포함하는 디지털 콘텐츠 식별 방법.

청구항5

제 1 항에 있어서,
상기 제 4 유일 식별자를 소정의 사용 조건들을 갖는 콘텐츠와 연관시키는 단계와,
상기 콘텐츠를 플레이하기 전에 제 4 유일 식별자를 인덱싱함으로써 사용 조건들을 검토하는 단계를 더 포함하는 디지털 콘텐츠 식별 방법.

청구항6

제 1 항에 있어서, 상기 제 4 유일 식별자 생성 단계는,
비인증된 액세스를 방지하기 위하여 템퍼 레지스턴트(temper-resistant) 환경에서 제 4 유일 식별자를 생성하는 단계를 포함하는 디지털 콘텐츠 식별 방법.

청구항7

사용자 장치에서의 디지털 콘텐츠의 사용을 추적하는 시스템에 있어서,

디지털 콘텐츠 —상기 콘텐츠는 이와 연관된 유일 콘텐츠 식별자를 포함함—를 컴퓨터 판독가능 매체를 거쳐 사용자에게 배포하는 다수의 콘텐츠 사이트들과,

디지털 콘텐츠 데이터를 사용자에게 플레이시키기 위한 인가들(licenses) —상기 인가들은 트랜잭션을 유일하게 식별하는 유일 트랜잭션 식별자와, 상기 트랜잭션에서 적어도 하나의 아이템을 유일하게 식별하는 유일 아이템 식별자를 포함함—를 부여하는, 각 전자 스토어가 네트워크와 결합된 다수의 전자 스토어들, 및

콘텐츠 데이터를 플레이하는 다수의 콘텐츠 플레이어들 —상기 각 디지털 콘텐츠 플레이어는 사용자들중 한명에게 인가된 상기 디지털 콘텐츠 데이터를 네트워크로부터 수신하고, 상기 콘텐츠 플레이어들은, 상기 콘텐츠 식별자, 상기 트랜잭션 식별자 및 상기 아이템 식별자의 수학적 조합에 기초하여 구매 식별자를 생성함—

을 포함하는 디지털 콘텐츠 사용 추적 시스템.

청구항8

제 7 항에 있어서,

상기 수학적 조합은 연결인 디지털 콘텐츠 사용 추적 시스템.

청구항9

제 7 항에 있어서,

상기 콘텐츠 플레이어는 템퍼 레지스턴트 환경을 포함하고, 상기 구매 식별자는 비인증된 액세스를 방지하기 위하여 템퍼 레지스턴트 환경에서 생성되는 디지털 콘텐츠 사용 추적 시스템.

청구항10

디지털 콘텐츠를 유일하게 식별하기 위한 디지털 콘텐츠 플레이어에 있어서,

콘텐츠 제공자로부터 수신된 콘텐츠를 유일하게 식별하는 제 1 식별자를 수신하는 수단과,

상기 콘텐츠가 수신되는 트랜잭션을 유일하게 식별하는 제 2 식별자를 수신하는 수단과,

상기 콘텐츠가 수신되는 트랜잭션에서의 아이템을 유일하게 식별하는 제 3 식별자를 수신하는 수단, 및

상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자의 수학적 조합에 기초하여 제 4 유일 식별자를 생성하는 수단을 포함하는 디지털 콘텐츠 플레이어.

청구항11

제 10 항에 있어서, 상기 생성 수단은,

상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자의 연결에 기초하여 제 4 유일 식별자를 생성하는 수단을 포함하는 디지털 콘텐츠 플레이어.

청구항12

제 10 항에 있어서, 상기 제 2 식별자 수신 수단은,

상기 콘텐츠를 판매하는 스토어로부터 유일 식별자를 수신하는 수단을 포함하는 디지털 콘텐츠 플레이어.

청구항13

제 10 항에 있어서, 상기 제 3 식별자 수신 수단은,

콘텐츠를 판매하는 스토어로부터 유일 식별자를 수신하는 수단을 포함하는 디지털 콘텐츠 플레이어.

청구항14

제 10 항에 있어서,

상기 제 4 유일 식별자를 소정의 사용 조건들을 갖는 콘텐츠와 연관시키는 수단과,

상기 콘텐츠를 플레이하기 전에 상기 제 4 유일 식별자를 인덱싱함으로써 사용 조건들을 검토하는 수단을 더 포함하는 디지털 콘텐츠를 유일하게 식별하는 방법.

청구항15

추적을 통해 디지털 콘텐츠 플레이어상의 디지털 콘텐츠를 유일하게 식별하기 위한 프로그램 명령들을 포함한 컴퓨터 판독가능 매체에 있어서,

콘텐츠 제공자로부터 수신된 콘텐츠를 유일하게 식별하는 제 1 식별자를 수신하는 프로그램 명령과,

상기 콘텐츠가 수신되는 트랜잭션을 유일하게 식별하는 제 2 식별자를 수신하는 프로그램 명령과,

상기 콘텐츠가 수신되는 트랜잭션에서의 아이템을 유일하게 식별하는 제 3 식별자를 수신하는 프로그램 명령, 및
상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자의 수학적 조합에 기초하여 제 4 유일 식별자를 생성하는 프로그램 명령
를 포함하는 컴퓨터 판독가능 매체.

청구항16

제 15 항에 있어서, 상기 생성 프로그램 명령은,

상기 제 1 식별자, 상기 제 2 식별자 및 상기 제 3 식별자의 연결에 기초하여 제 4 유일 식별자를 생성하는 프로그램 명령을 포함하는
컴퓨터 판독가능 매체.

청구항17

제 15 항에 있어서, 상기 제 2 식별자 수신 프로그램 명령은,

상기 콘텐츠를 판매하는 스토어로부터 유일 식별자를 수신하는 프로그램 명령을 포함하는 컴퓨터 판독가능 매체.

청구항18

제 17 항에 있어서, 상기 제 3 식별자 수신 프로그램 명령은,

콘텐츠를 판매하는 스토어로부터 유일 식별자를 수신하는 프로그램 명령을 포함하는 컴퓨터 판독가능 매체.

청구항19

제 15 항에 있어서,

상기 제 4 유일 식별자를 소정의 사용 조건들을 갖는 콘텐츠와 연관시키는 프로그램 명령과,

상기 콘텐츠를 플레이하기 전에 상기 제 4 유일 식별자를 인덱싱함으로써 사용 조건들을 검토하는 프로그램 명령을 더 포함하는 컴퓨
터 판독가능 매체.

청구항20

제 15 항에 있어서, 상기 제 4 유일 식별자 생성 프로그램 명령은,

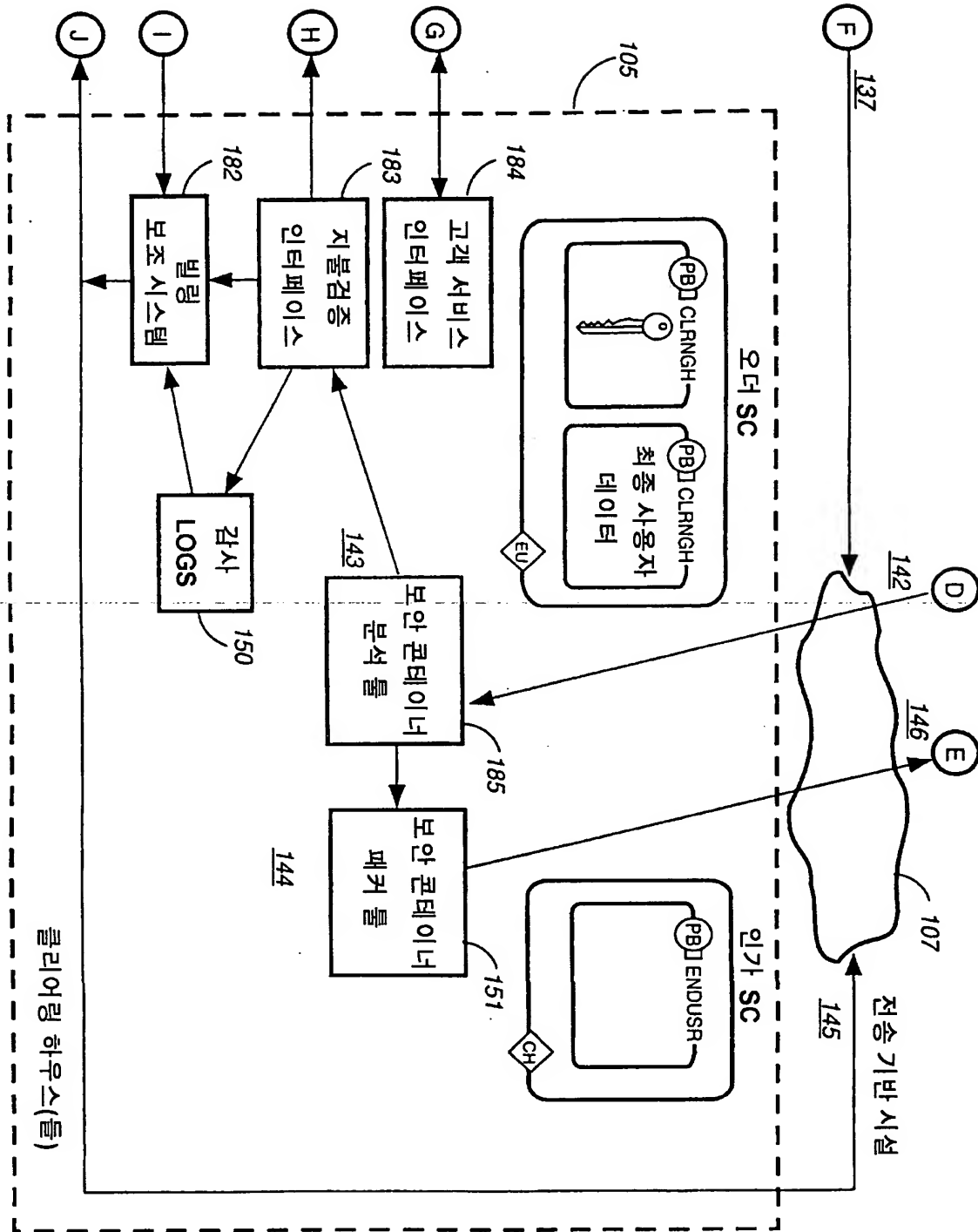
비인증된 액세스를 방지하기 위하여 템퍼 레지스트된 환경에서 제 4 유일 식별자를 생성하는 프로그램 명령을 포함하는 컴퓨터 판독
가능 매체.

도면

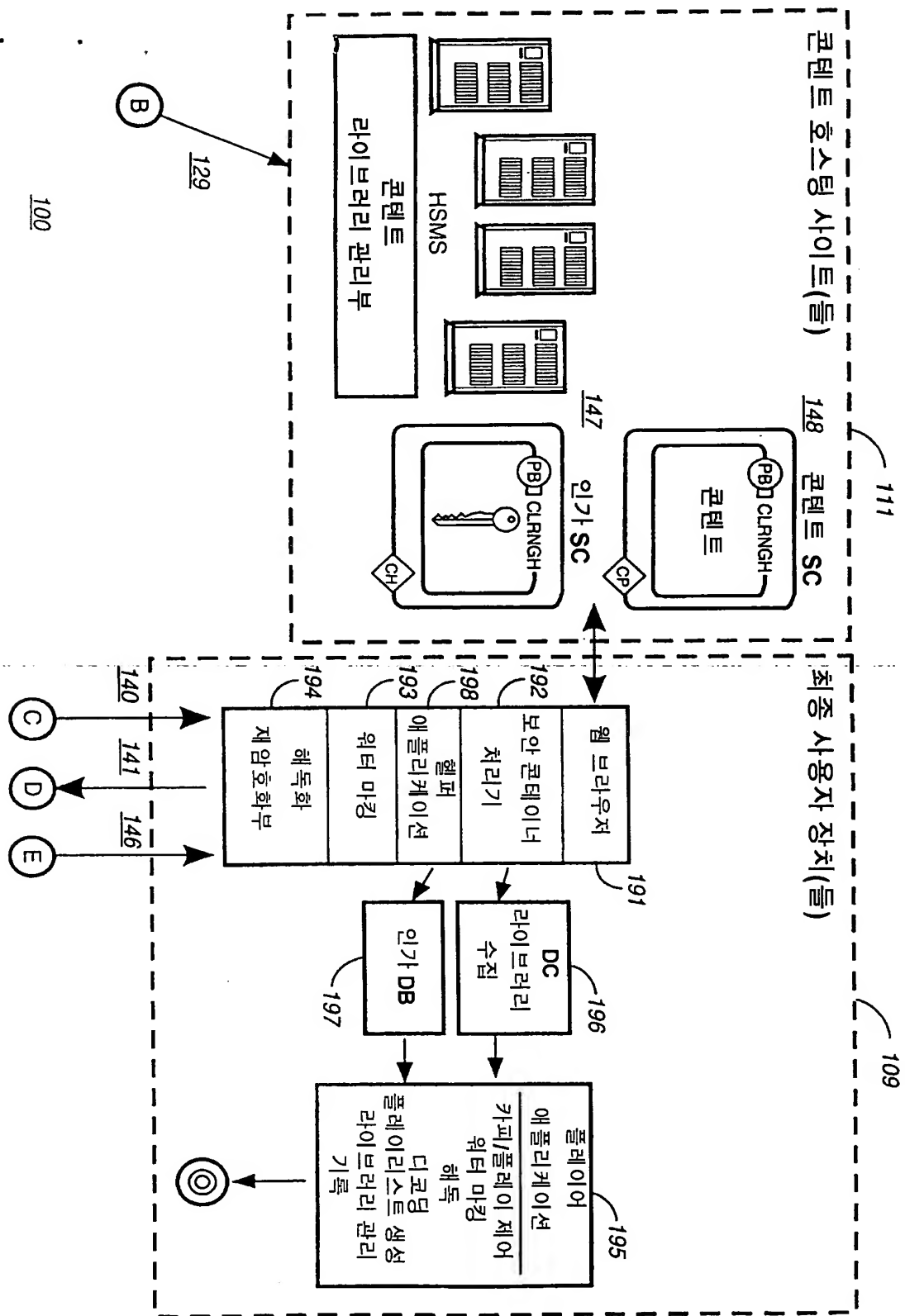
도면1a

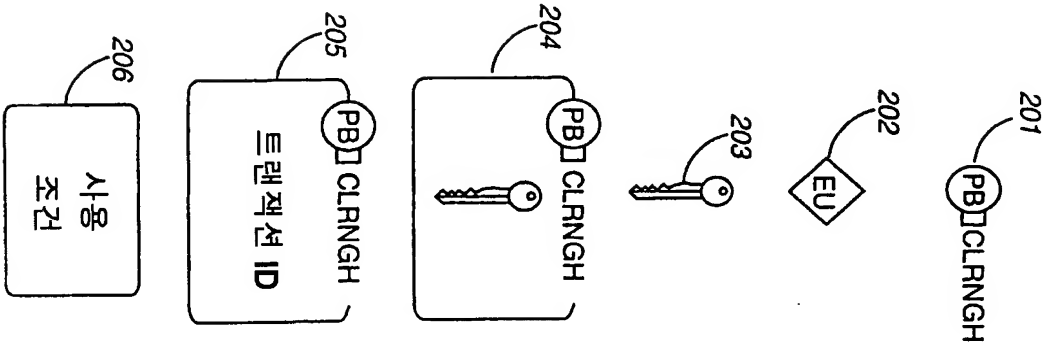
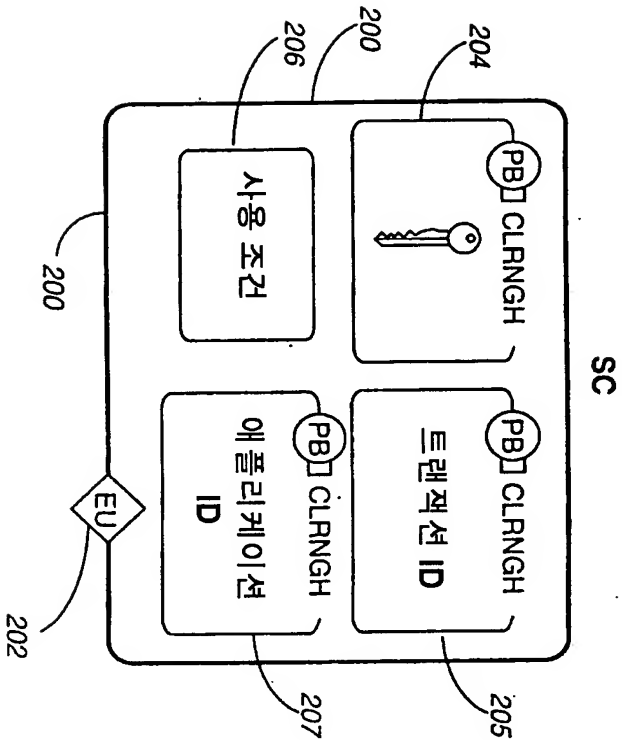




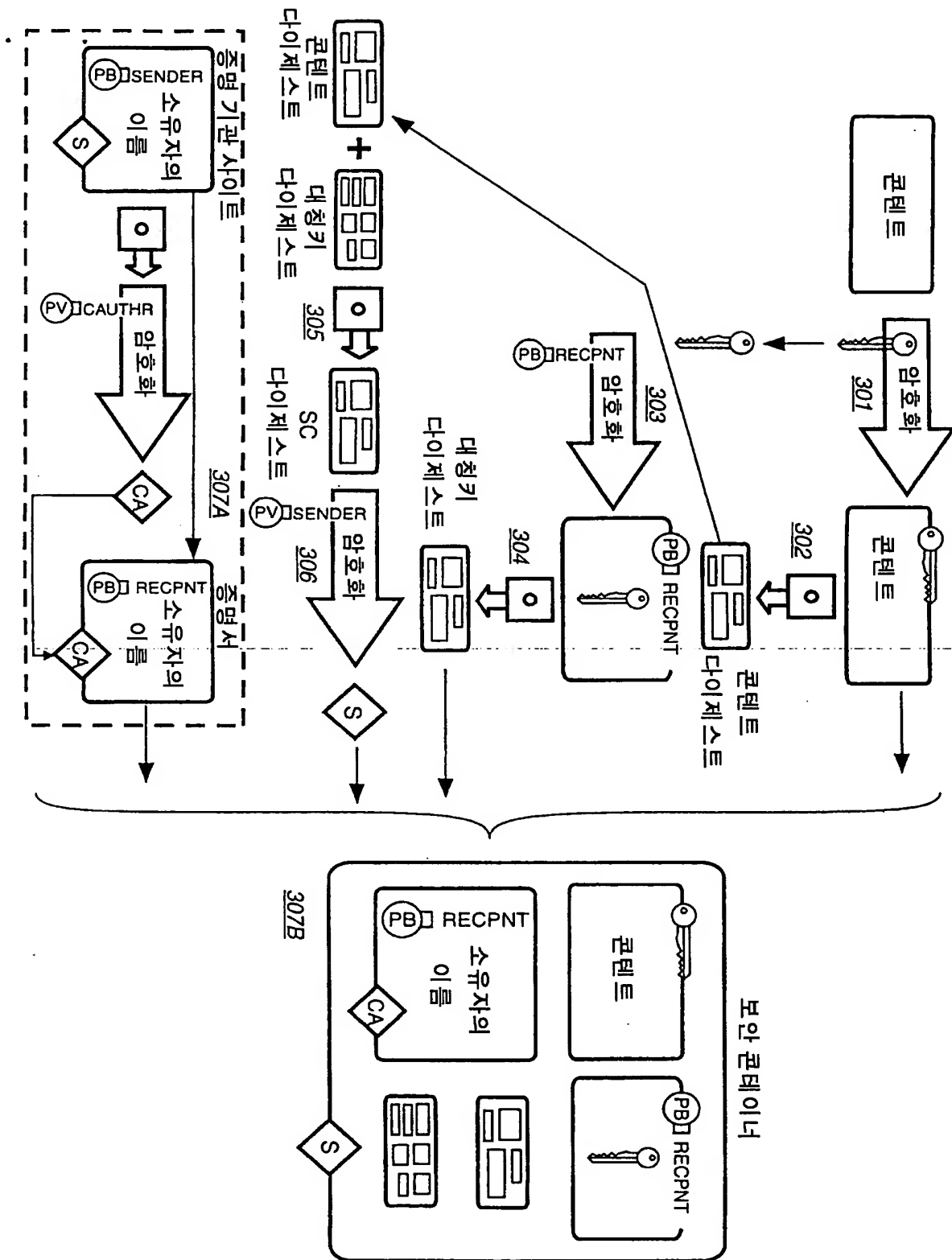


도면1d

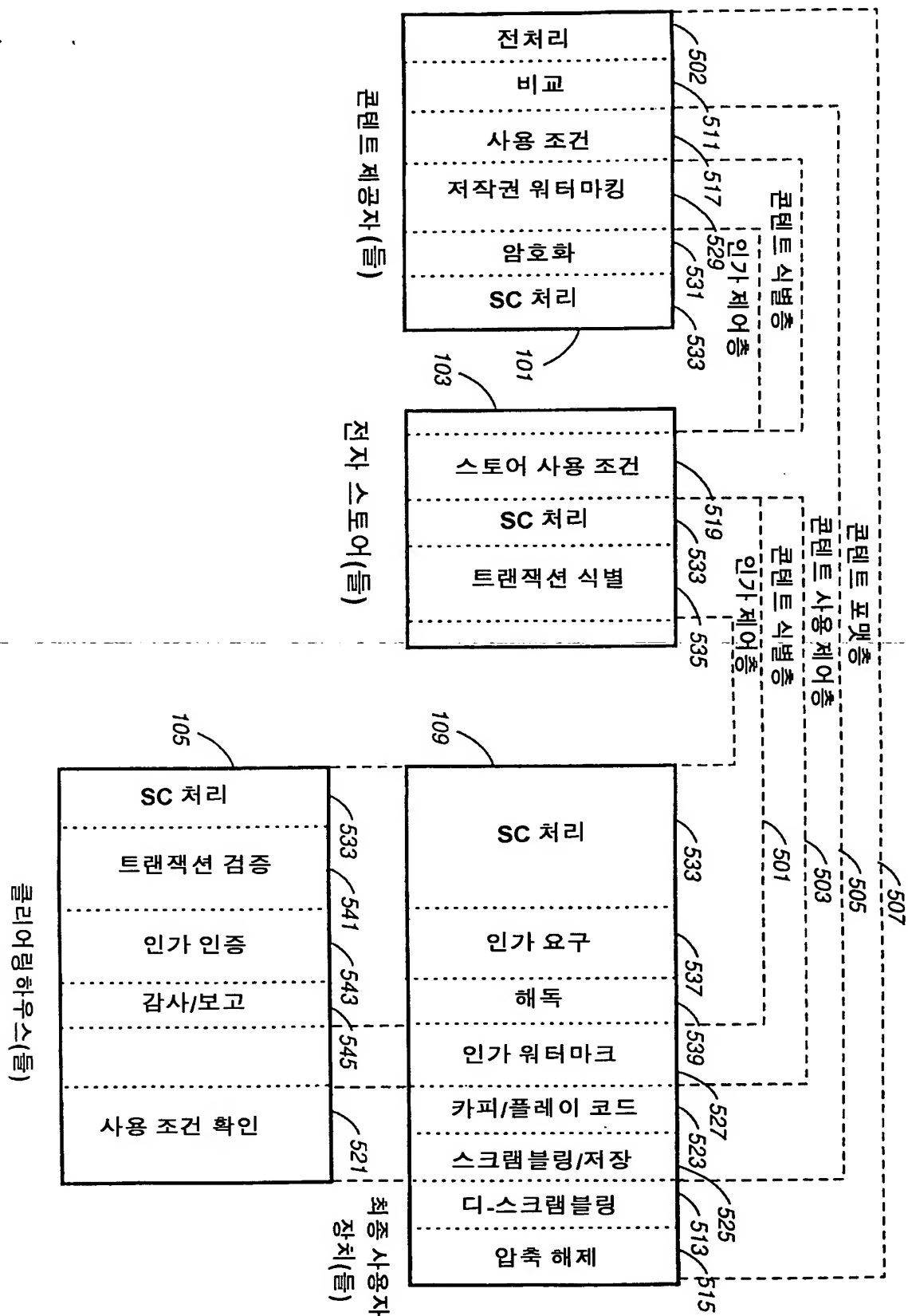




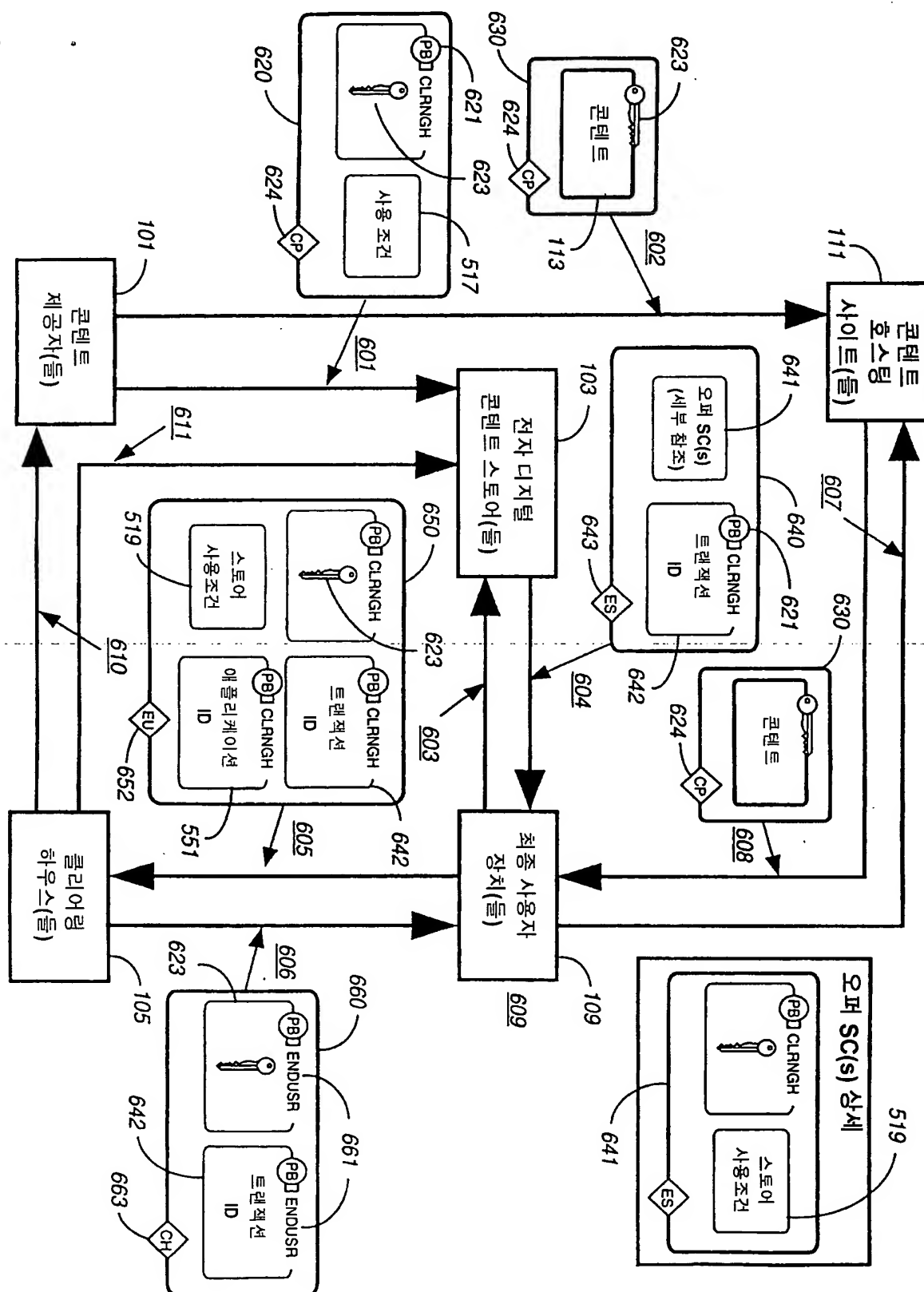
도면3



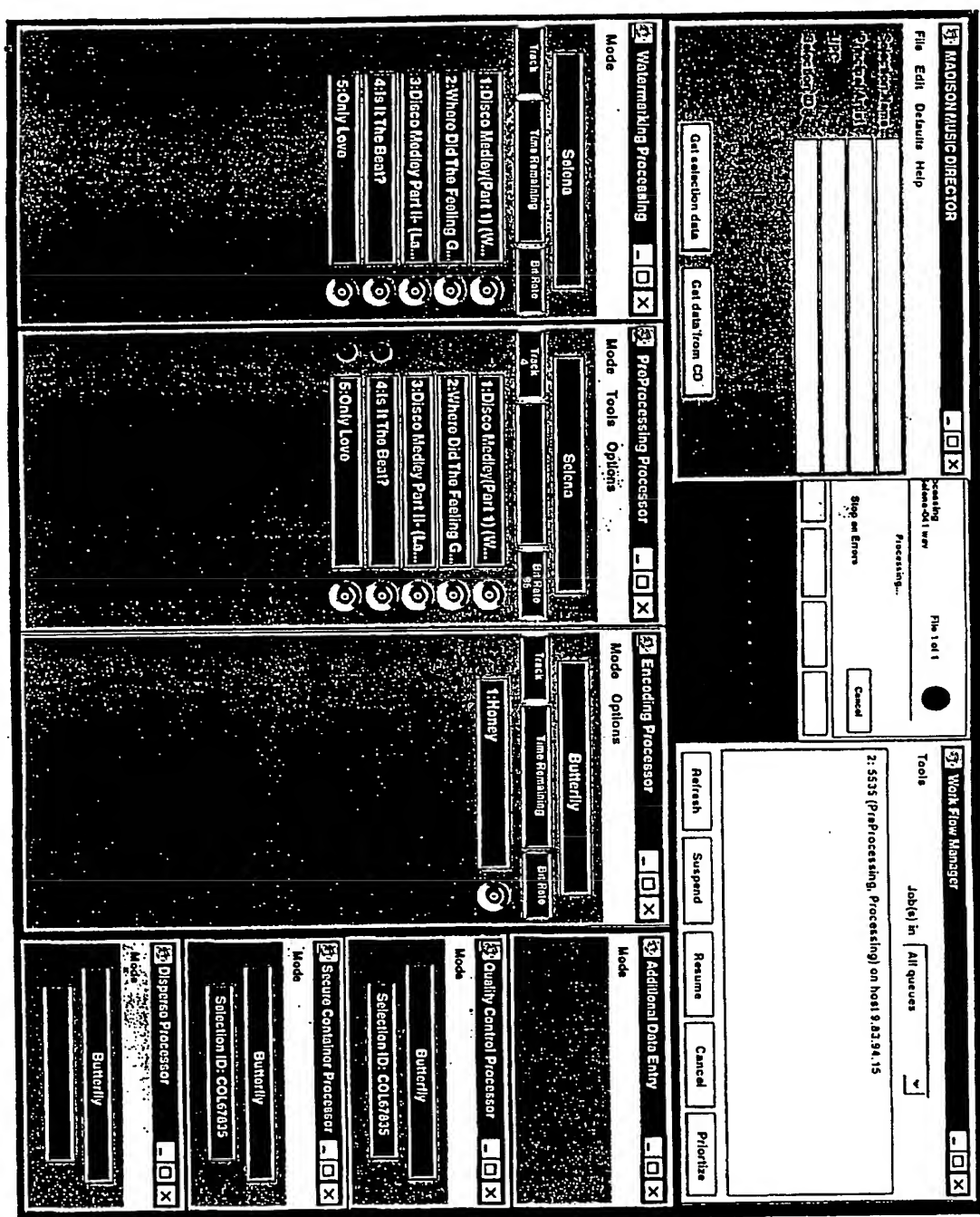




도면6

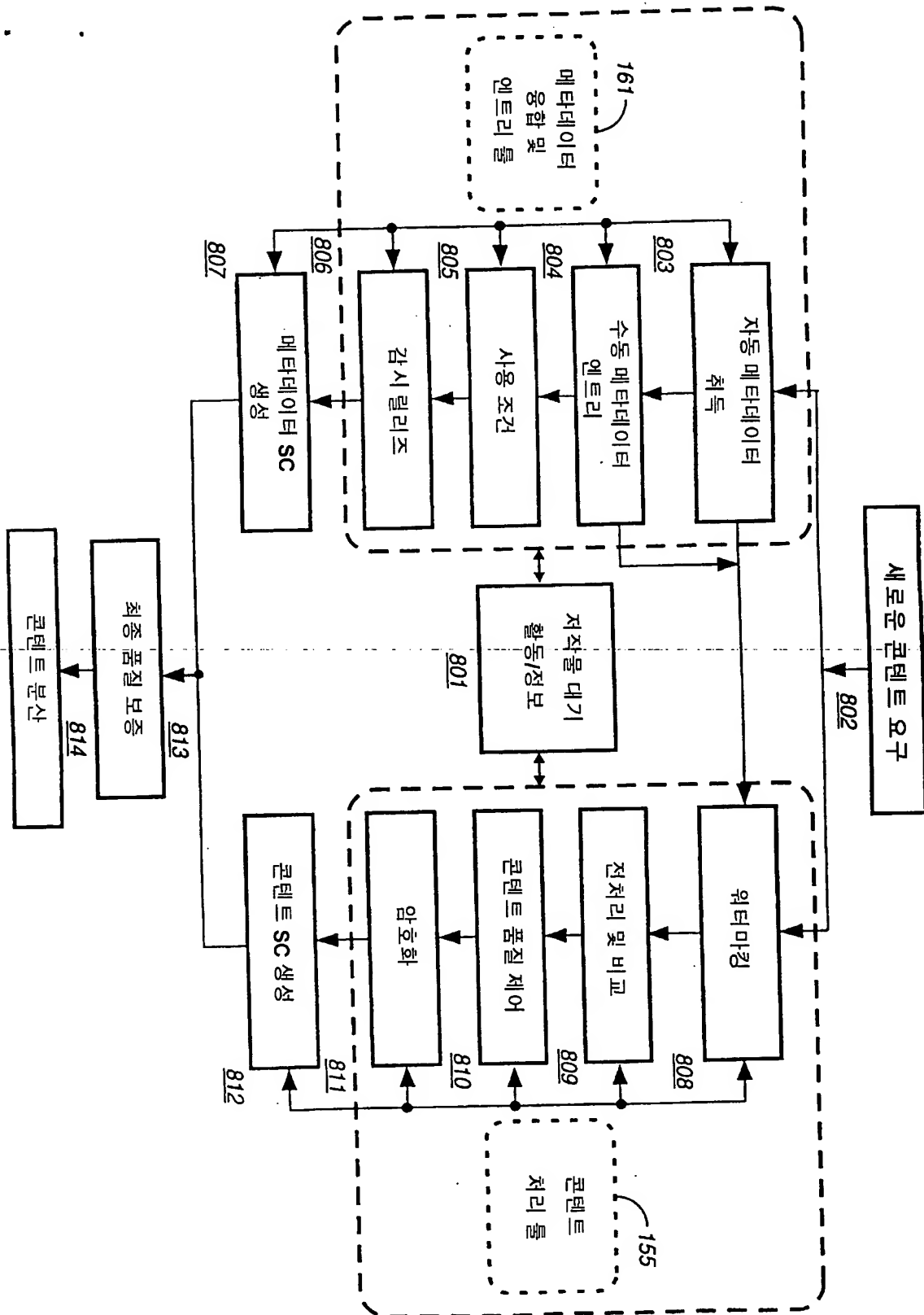


도면7

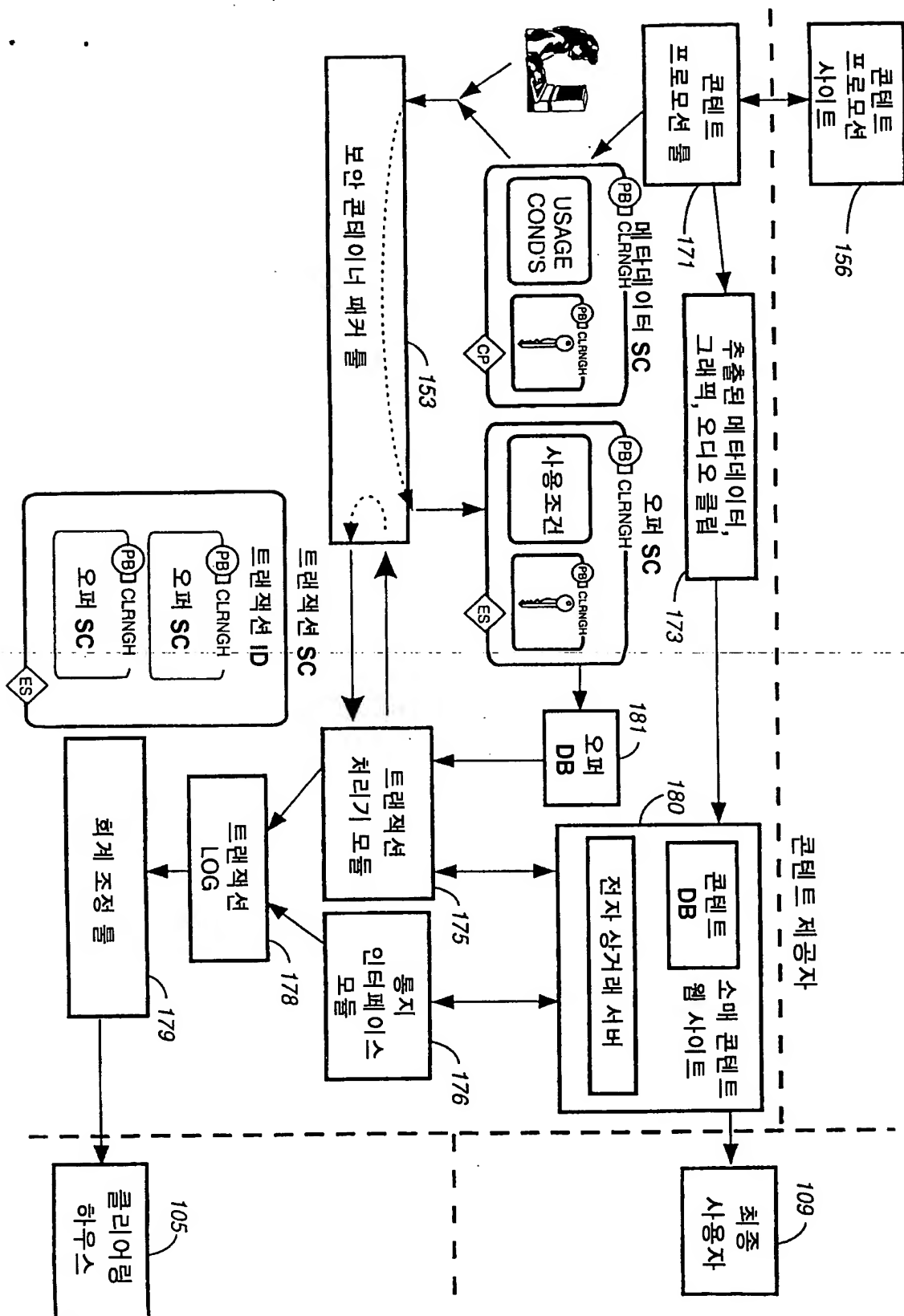


700

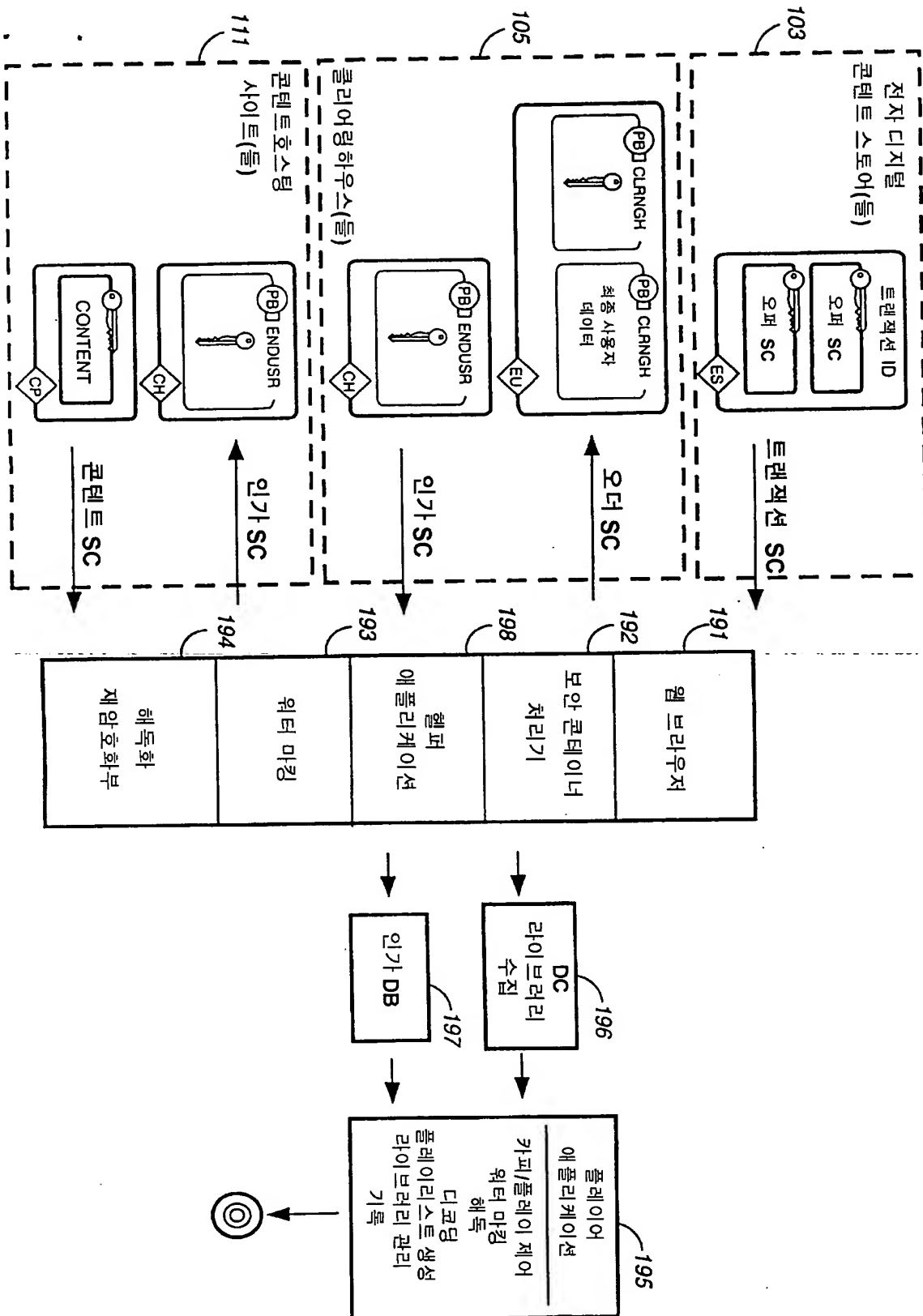
도면 8



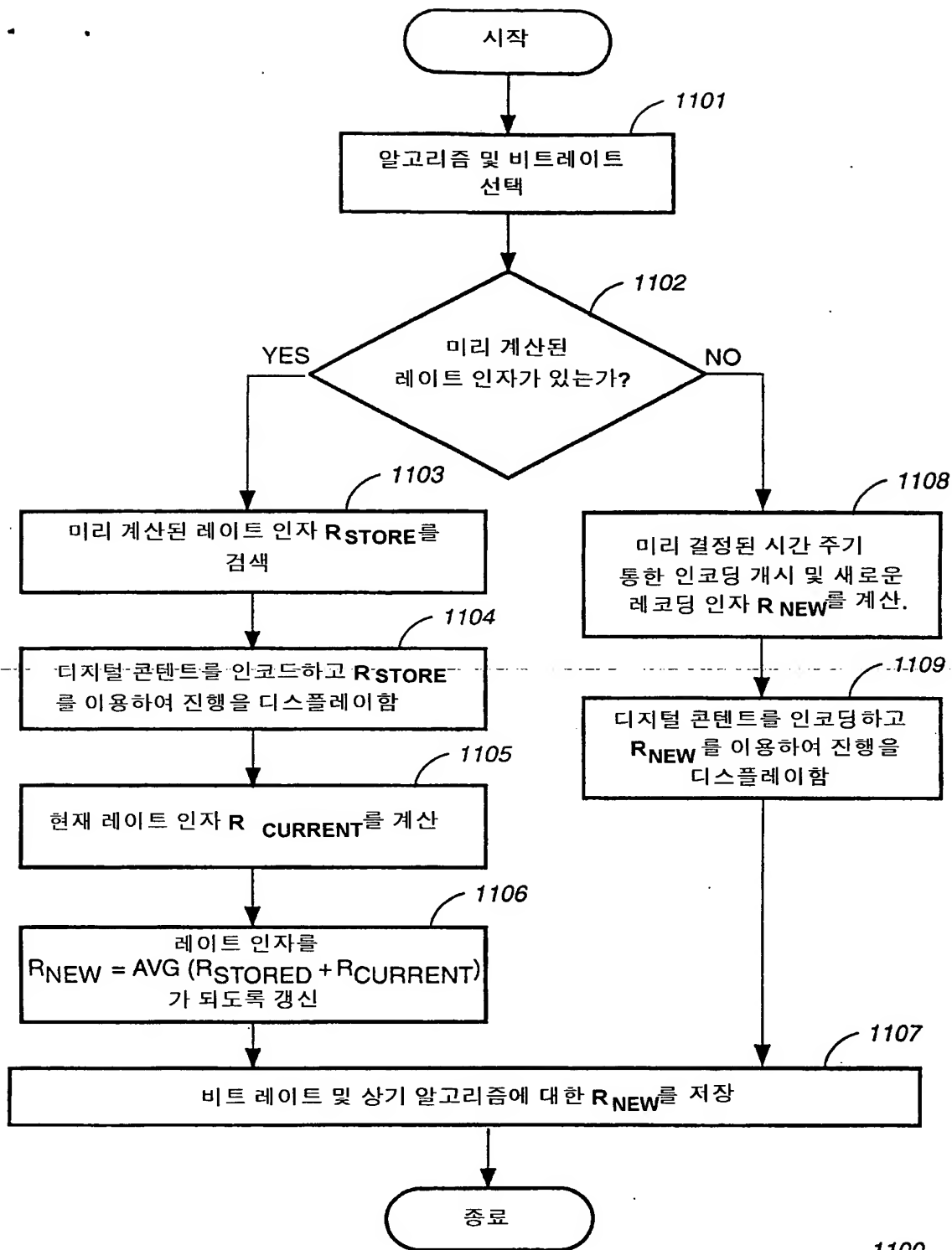
도면 9



도면10

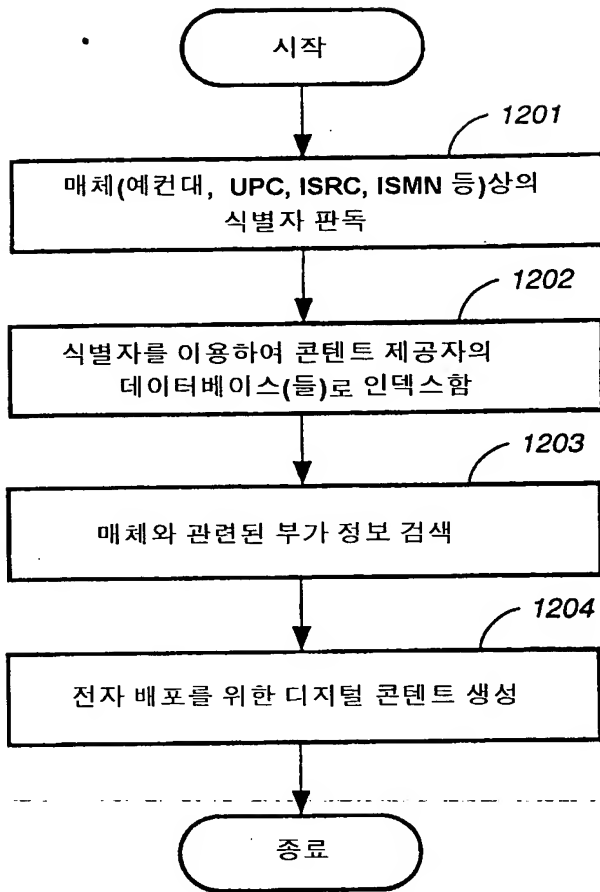


도면 11

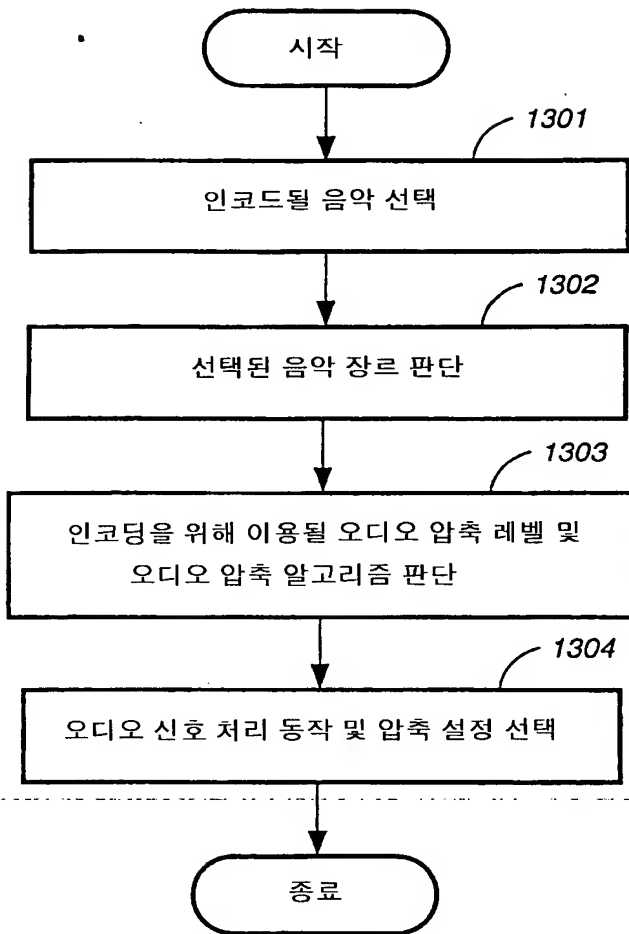


1100

도면12

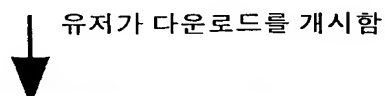


도면13

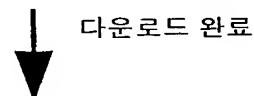


도면14

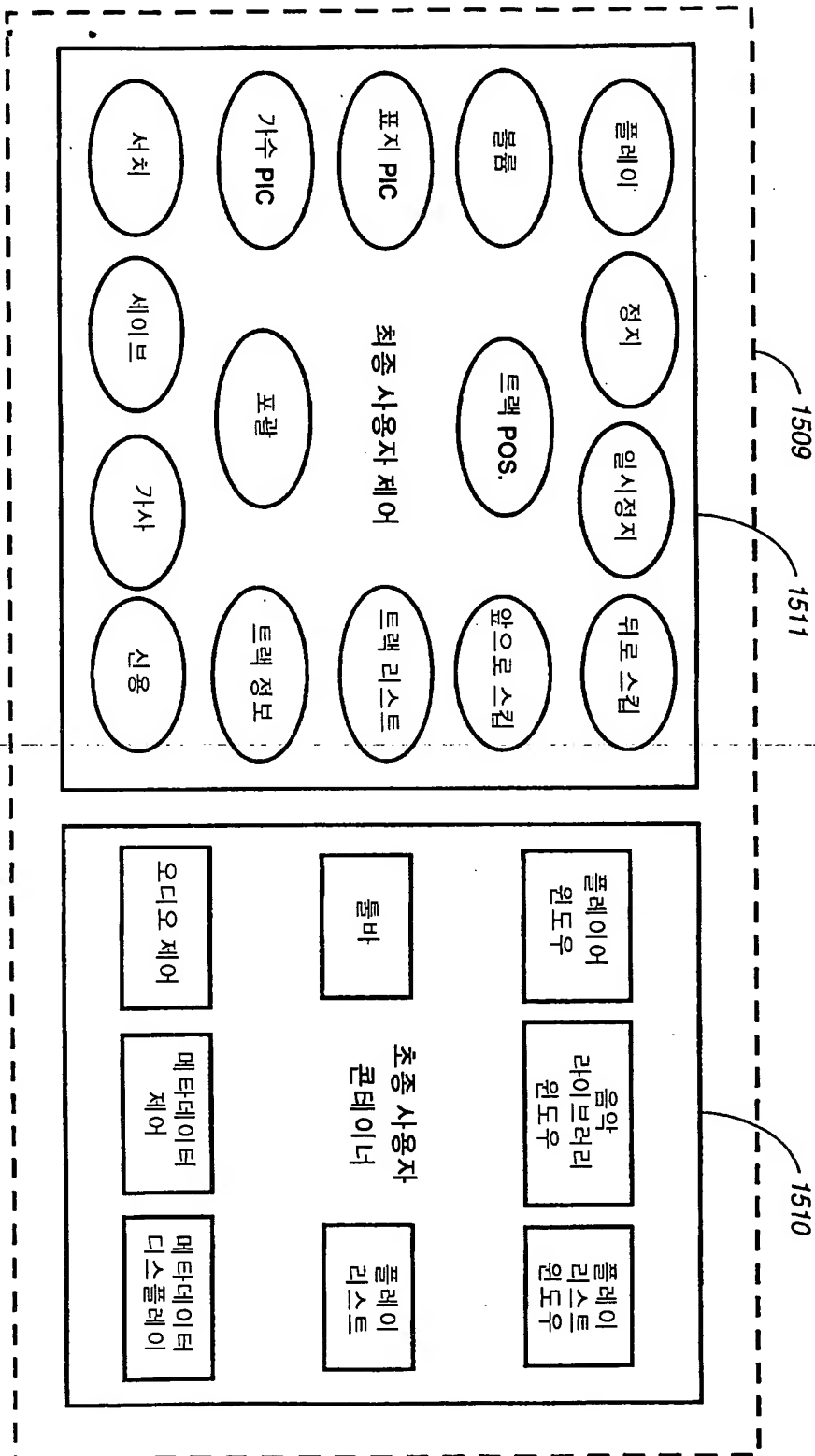
•



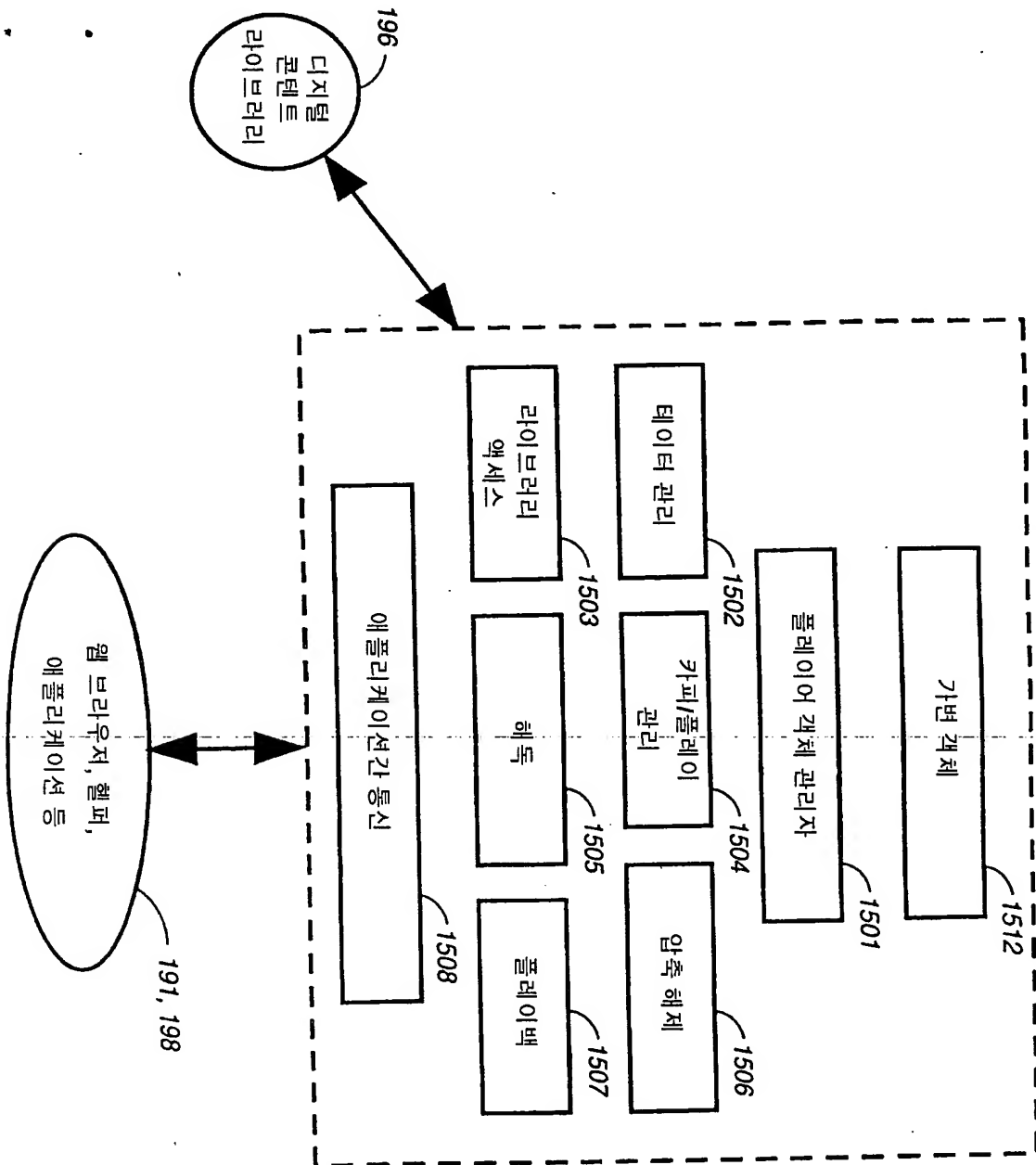
1



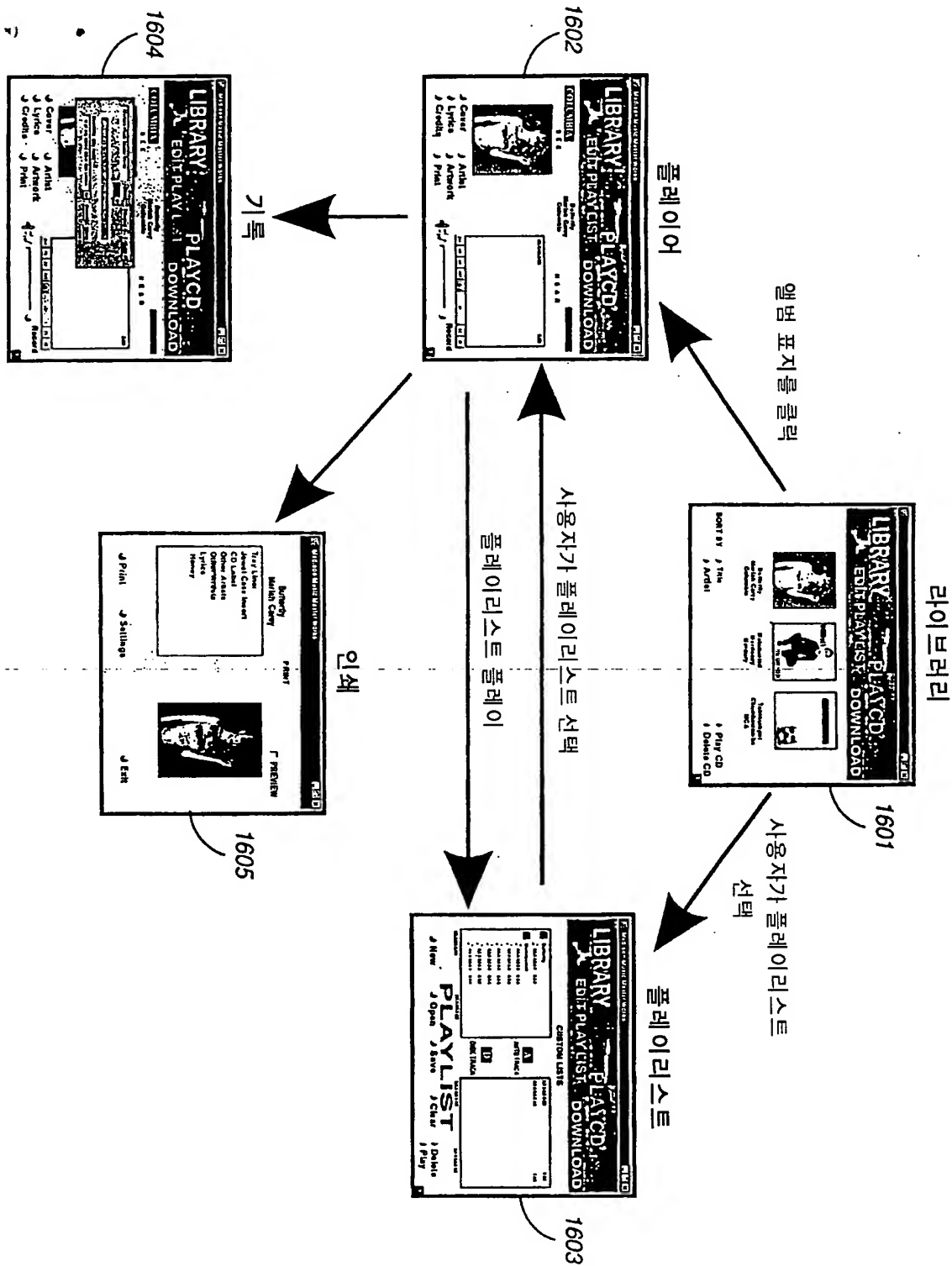
—



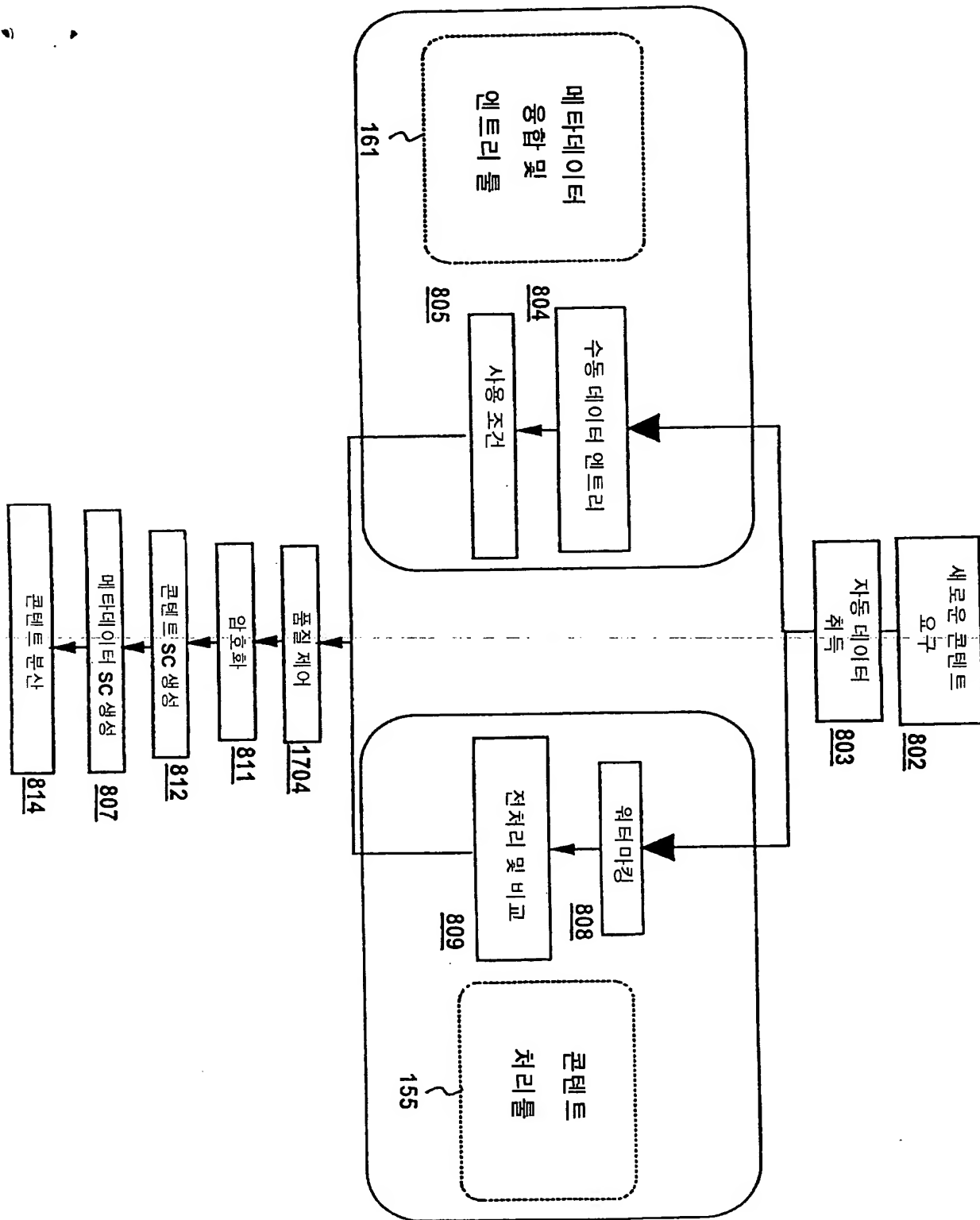
도면15b



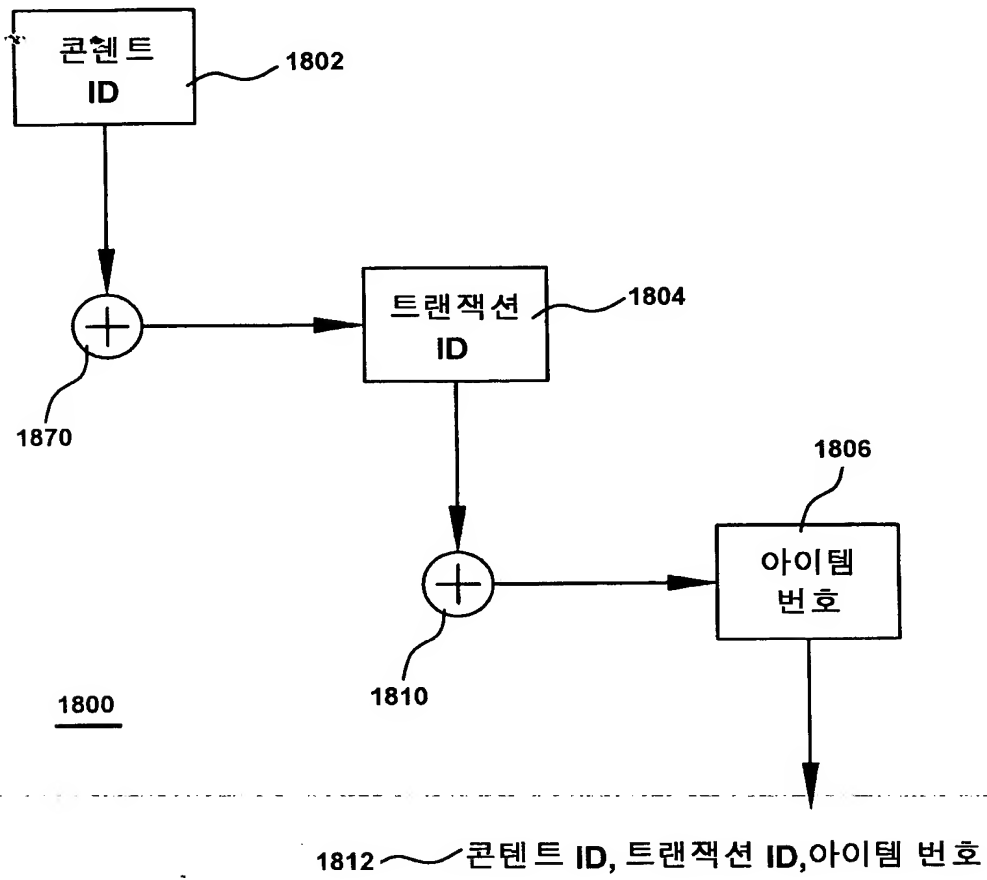
도면 16



도면17



도면 18



Publication No.: 10-2001-0034000

Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V.

ABSTRACT

Content information such as a movie, an audio file or a textual message is supplied to an end-user in a software object that has an encapsulated procedure for end-user access of the content information in a runtime environment. The object can specify time frame for and manner wherein the content information is to be accessed. Since the procedure is encapsulated in the object together with the content data, and since transport of the object over the Internet is done after serializing, an adequate degree of security is provided against unauthorized play-out or copying.

(19)대한민국특허청(KR)
(12) 공개특허공보(A)(51) Int. Cl. 6
G06F 17/60(11) 공개번호 특2001-0034000
(43) 공개일자 2001년04월25일

(21) 출원번호	10-2000-7007594		
(22) 출원일자	2000년07월10일		
번역문제출일자	2000년07월10일		
(86) 국제출원번호	PCT/EP1999/08333	(87) 국제공개번호	WO 2000/28398
(86) 국제출원출원일자	1999년11월01일	(87) 국제공개일자	2000년05월18일
(81) 지정국	EP 유럽특허 : 오스트리아, 벨기에, 스위스, 사이프러스, 독일, 덴마크, 스페인, 핀 랜드, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란 드, 포르투갈, 스웨덴, 국내특허 : 중국, 일본, 대한민국,		

(30) 우선권주장	09/189534 1998년11월10일 미국(US)
(71) 출원인	코닌클리케 필립스 일렉트로닉스 엔.브이. 요트.게.아. 룰페즈 네덜란드왕국, 아인드호펜, 그로네보르스베그 1
(72) 발명자	슈테인 예브게니 네덜란드 5656 아아 아인트호벤, 프로페써 홀스틀란 6
(74) 대리인	이화익

심사청구 : 없음

(54) 저작권 보호를 위해 소프트웨어 객체로서 제공된 콘텐츠

요약

영화, 오디오 파일 또는 텍스트 메시지와 같은 콘텐츠 정보가, 런타임 환경에서 콘텐츠 정보의 최종 사용자의 액세스를 위한 캡슐화 된 프로시저를 갖는 소프트웨어 객체로 최종 사용자에게 제공된다. 이 객체는, 콘텐츠 정보가 액세스되는 시간 프레임과 방식을 지정할 수 있다. 콘텐츠 데이터와 함께, 프로시저가 객체 내부에 캡슐화되고, 인터넷을 통한 객체의 전송이 직렬화 이후에 이루어지기 때문에, 권한이 없는 재생 또는 복제를 방지하는 적절한 보안성이 제공된다.

대표도

도1

색인어

저작권, 콘텐츠, 런타임, 프로시저, 객체, 직렬화, 분산 소프트웨어, 자바

명세서

본 발명은, 특히, 민수용 전자장비 또는 멀티미디어 컴퓨터의 최종 사용자에게 제공된 콘텐츠 데이터에 대한 통제된 액세스를 제공하는 방법에 관한 것이다. 또한, 본 발명은, 디지털 데이터 콘텐츠의 권한이 없는 복제를 방지하는 방법에 관한 것이다.

본 명세서에서 사용되는 용어 "콘텐츠" 또는 "콘텐츠 데이터"는, 예를 들면, 문자숫자식 텍스트, 그래픽, 비디오, 오디오, 멀티미디어 등과 같이, 최종 사용자를 위한 정보를 포함하는 데이터를 칭한다.

현재, 디지털 콘텐츠는 일반적으로 케이블이나 인터넷을 사용하여 원격지 서버로부터 최종 사용자에게 전송되거나 스트림 전송되거나, DVD 등 위에 제공된다. 콘텐츠는 수신장치(예를 들면, 컴퓨터, 셋톱 박스)에 의해 처리되어, 사용자에게 표시된다. 콘텐츠는 "워터마킹"을 사용하여, 즉 사용자에게 의해 감지될 수 없지만 재생 또는 검증 소프트웨어나 하드웨어에 의해 인식되는 디지털 변형을 추가하여 저작권 보호가 이루어질 수 있다. 콘텐츠를 보호하는 또 다른 방법은 암호화이다. 콘텐츠 데이터는, 데이터를 그것의 목적지로 전송하기 전에 특수한 암호화 알고리즘을 사용하여 인코딩된다. 목적지 장치 또는 중간 프로세서(PC, 케이블 박스, 셋톱 박스 등)

에서, 이 스트림은 재생 또는 저장되기 전에 암호해제된다.

그러나, 이들 방법과 관련하여 다수의 문제점이 존재한다. 워터마킹은, 예를 들어, 콘텐츠 변형에 매우 민감하다. 디지털 콘텐츠가 "워터마크"가 알지 못하는 소프트웨어/하드웨어에 의해 변형되면, 이 워터마크는 원래의 형태로 지속되는 것이 보장되지 않는다. 예를 들면, 화상의 사이즈 변화, 화상을 다른 파일 포맷으로 저장하는 것, 압축기술을 적용하는 것 등은 워터마크에도 영향을 미치며, 그것을 덜 유용하게 만든다. 암호화 기법 역시 다수의 문제점을 제공한다. 컴퓨터/프로세싱 하드웨어와 소프트웨어가 더욱 강력해지고 복잡해짐에 따라, 알려진 알고리즘은 "암호가 풀어져", 쓸 수 없게 된다. 또 다른 문제점은 표준화이다. 즉, 다수의 판매자와 대중 시장을 다루기 위해서는, 콘텐츠 보호 방법이 표준화될 필요가 있다. 반면에, 표준 암호화 기법은 비교적 빨리 사용이 불가능하게 되며, 전문가에게 알려지므로, 깨뜨리기가 쉬워진다.

결국, 본 발명의 목적은, 콘텐츠 데이터의 통제된 액세스를 제공하는 또 다른 방법을 제공함에 있다. 본 발명의 또 다른 목적은, 권한이 없는 행위자에 의해 디지털 콘텐츠를 복제 또는 재생하기가 더욱 어렵게 만드는데 있다. 본 발명의 또 다른 목적은, 디지털 콘텐츠 분배의 안전하고도 미래와의 호환이 가능한 방법을 제공함에 있다.

상기한 목적을 위해, 본 발명은, 한 개 또는 그 이상의 소프트웨어 객체로서, 바람직하게는 네트워크를 통해, 콘텐츠 정보를 제공하거나 수신하는 방법을 제공한다. 프로시저는 런타임 환경에서 정보의 액세스를 위한 객체 내부에 캡슐화된다. 즉, 최종 사용자에게 의해 정보를 액세스하기 위한 프로시저는, 콘텐츠 정보와 함께 패키징되어, 최종 사용자에게 전달된다.

공지된 것과 같이, 소프트웨어 객체는, 콘텐츠 데이터와 이 데이터를 처리하기 위한 메소드 또는 프로시저를 포함한다. 객체지향 프로그래밍에 있어서, 메소드는, 클래스의 일부로서 정의되고 클래스의 임의의 객체 내부에 포함하는 프로그래밍된 프로시저에 해당한다. 한 개의 객체는 한 개 이상의 메소드를 가질 수 있다. 객체 내부의 메소드는 그 객체에게 알려진 데이터에만 액세스할 수 있는데, 이것은 어플리케이션에 있는 객체들의 집합 중에서 데이터 무결성을 확보하게 한다.

COM 또는 DCOM 기술에 기반을 둔 HAVi, 자바/지니(JINI), 홈 API, CORBA 또는 기타 기술과 같은 개방형 분산 소프트웨어 아키텍처는 네트워크(인터넷, 홈 네트워크, 근거리 통신망, 광대역 통신망 등)를 통해 소프트웨어 객체의 전송을 허용한다. 소프트웨어 표시, HAVi, COM 기술의 사용과 OLE 자동 객체에 대한 더욱 상세한 정보를 위해, 다음과 같은 특허 문헌을 참조를 위해 본 명세서에 통합한다: Paul Chambers and Saurabh Srivastava의 10/15/96 출원된 미국 특허출원 제 08/731,624호(변호사 사건번호 PHA 23,169)인 "TASK-DRIVEN DISTRIBUTED MULTIMEDIA CONSUMER SYSTEM"; Yevgeniy Shteyn의 9/2/98 출원된 미국 특허출원 제 09/146,020호(변호사 사건번호 PHA 23,492)인 "LOW DATA-RATE NETWORK REPRESENTED ON HIGH DATA-RATE HAVI-NETWORK"; Yevgeniy Shteyn의 10/2/98 출원된 미국 특허출원 제 09/165,683호(변호사 사건번호 PHA 23,483)인 "CALLS IDENTIFY SCENARIO FOR CONTROL OF SOFTWARE OBJECTS VIA PROPERTY ROUTES"; Yevgeniy Shteyn의 10/2/98 출원된 미국 특허출원 제 09/165,682호(변호사 사건번호 PHA 23,484)인 "CONTROL PROPERTY IS MAPPED ONTO MODALLY COMPATIBLE GUI ELEMENT"; Yevgeniy Shteyn과 Gregory Gewickey의 6/30/98 출원된 미국 특허출원 제 09/107,525호(변호사 사건번호 PHA 23,438)인 "DYNAMIC DE-REGISTERING OF DEVICES IN SYSTEM WITH MULTIPLE COMMUNICATION PROTOCOLS".

장치로 전송되었을 때, 이와 같은 소프트웨어 객체는 그것의 시스템 소프트웨어와 상호작용할 수 있다. 예를 들어, HAVi DCM은 FAV로 업로드되어, 자바 런타임 환경에서 실행될 수 있다. DCM은, 그래픽, 오디오, 비디오, 텍스트, 이미지 등의 재생, 저장, 기록 및 기타의 처리에 대한 API를 구현하도록 프로그래밍될 수 있다. 이와 같은 경우에, 소프트웨어 객체는 종간의 암호해제나 변형이 없이 재생장치와 직접 작용한다. 모든 동작은 객체 그 자체에 의해 제어되며, 적대적인 어플리케이션으로부터 숨겨진다. 콘텐츠가 저장될 필요가 있을 때, 객체 제어된 저장 API가 호출된다(예를 들면, 직렬화, 이하의 내용을 참조할 것). 객체가 저장(기록) 과정을 제어하기 때문에, 호스트 시스템은 저장된 콘텐츠를 액세스하기 위해 객체를 재생성해야 하므로, 그것의 콘텐츠가 보호된다. 객체는, 기록물의 품질, 콘텐츠가 기록되거나 재생될 수 있는 횟수와, 호스트 시스템과의 기타 상호작용에 영향을 미칠 수 있다. 소프트웨어 객체는 시간에 민감하도록 만들어질 수 있다. 예를 들면, 영화 객체는 전용으로 사용될 수 있는데, 즉 그것의 재생 API가 특정한 양의 시간, 즉 영화 재생 시간, 일자 등의 동안에만 사용될 수 있다. 제어 객체는 모든 콘텐츠를 포함할 필요는 없다. 콘텐츠가 매우 클 때, 객체는 콘텐츠 위치에 대한 기준값(들) 만을 유지하고, 필요에 따라 검색을 할 수 있다. 필요하거나 바람직한 경우에, 복수의 객체로 구성된 체인이 동작을 제어할 수 있다. 예를 들면, 서로 다른 영화 장면이 서로 다른 객체에 의해 제어된다. 객체는, 콘텐츠의 특정한 부분에 대한 자유로운 (시도) 액세스를 제공하고 다른 부분에 대해 지불을 요구하도록 설정될 수 있다. 사용자의 선호에 근거한, 시스템 자원과의 조건부 상호작용이 달성될 수 있다. (예를 들면, 가입을 통해) 사용자 액세스의 레벨에 의존하여, 광고와 판촉이 별개의 객체로서 삽입될 수 있다.

장치와 객체의 상호작용 이후에, 타겟 클라이언트의 실행 환경이 알려지거나 검출될 수 있는 경우에, 객체는 이진 코드를 감출 수 있다. 예를 들면, 더 우수한 재생 알고리즘 또는 이진 업그레이드가 자바 VM을 실행하는 TriMedia 머신으로 전달될 수 있다.

객체를 통해 최종 사용자에게 데이터 콘텐츠를 전달하는 제시된 방법은, 저작권 보호 외에 다른 용도에 대해서도 매우 적합하다. 예를 들면, 전자메일, (전화를 통한) 원격회의 또는 화상회의는 안전 문제로 인해 소프트웨어 객체의 교환에 기반을 둘 수 있다. 마찬가지로, 전자 금융 거래는 소프트웨어 객체의 통신을 통해 안전하게 될 수 있다. 전자 메일은 소프트웨어 객체로서 구현될 수 있다.

예를 들면, 서버로부터 클라이언트로의 네트워크를 통한 객체의 전송은, 예를 들면, 객체 직렬화를 통해 달성된다. 자바에서의 객체 직렬화는, 객체 또는 이들로부터 도달될 수 있는 객체의 복수의 바이트로 구성된 스트림으로의 인코딩을 지원하며, 스트림으로부터

의 객체 그래프의 보완적인 재구성을 지원한다. 직렬화는, 라이트웨이트(lightweight) 지속성을 위해 사용되며 소켓 또는 원격 방법 호출(Remote Method Invocation: RMI)을 통한 통신에 사용된다. 객체의 초기값 디코딩은 개인 및 비상주 데이터를 보호하고, 클래스의 진화를 지원한다. 적대자에 의해 표절되고 복제될 수 있는 분리된 디지털 데이터 스트림은 전통적인 의미에서는 존재하지 않는다. 전송되는 것은 단지 복수의 비트로 구성된 스트링으로, 프로시저와 콘텐츠 정보가 스트림으로부터 인식할 수 없으므로, 일반인이 그것의 의미에 대한 실마리를 발견하는 것은 불가능하다. 클래스는, 안전성을 높이기 위해 그 자신의 외부 인코딩을 실현할 수 있으며, 외부 포맷에 대해서만 책임이 있다(출처: <http://www.javasoft.com/products/jdk/1.1/docs/guide/serialization/index.html>). 따라서, 암호화된 콘텐츠 데이터와 함께, 암호해제 프로시저와 객체 내부에 캡슐화될 수 있다. 그 후, 암호해제 프로시저가, 가능한 경우에는 수신자의 ID, 암호해제 키, 또는 재생장치의 일련 번호 등을 검증하는 캡슐화된 검증 프로시저와 보완하여, 수신단에서 호출된다.

간략을 기하기 위해, 인터넷을 통한 애플릿(Applet)의 다운로드가 알려져 있다. 애플릿에 대한 사용자의 액세스에는 수신하는 클라이언트에 상주하는 브라우저 어플리케이션이 필요하다. 브라우저 또는 플러그인은 애플릿의 부분이 아니다. 본 발명에 있어서는, 소프트웨어 객체가 그 자신의 프로시저를 사용하여 수신측의 런타임 환경(예를 들면, HAVi 런타임, 홈 API 런타임[=윈도우즈 OS], 지니 런타임)에서 바로 활성화되며, 런타임 내부의 브라우저나 다른 클라이언트 어플리케이션을 필요로 하지 않는다.

본 발명의 다양한 바람직한 발명내용이 첨부된 청구범위와 그것의 가능한 조합에 기재되어 있다. 예를 들면, 화상회의 시스템은, 통상적인 비디오 스트리밍과 객체 캡슐화된 안전한 오디오 및/또는 그래픽 데이터를 제공할 수 있다.

이하, 본 발명은 다음의 첨부도면을 참조하여 더욱 상세히 설명한다:

도 1-도 5는 본 발명의 방법이 구현되는 시스템의 예에 대한 블록도이다.

전체 도면을 통해, 동일한 도면부호는 유사하거나 대응하는 특징부를 나타낸다.

도 1은 본 발명의 방법을 구현하는 HAVi 시스템(100)의 블록도이다. 시스템(100)은, 저장매체(102)와, 본 실시예에 있어서는 디지털 TV를 포함하는 FAV(Full AV mode)(104)를 구비한다. FAV(104)는, 자바 가상머신(106)이다. 저장매체(102)는, 예를 들어, 재생 API(112)에 의해 나타낸 콘텐츠 데이터(110)와 재생 프로시저와 함께, 예를 들면 직렬화 제거 이후에 외부 시스템(100)으로부터, 또는 본 발명에서는 HAVi DCM(108)인 소프트웨어 객체를 포함하는 DVD 또는 기타 물리 데이터 매체로부터 전자적으로 수신된 소프트웨어 객체(108)를 저장하는 버퍼를 구비한다. 소프트웨어 객체(108)는 FAV(104) 상의 재생 프로세스로 업로드되어, API가 직접 자바 VM(106)과 상호작용하도록 한다. 콘텐츠에 대한 조건부 액세스는, 보안 또는 사용자/시스템 능력에 기반을 둘 수 있다. 보안에 기반을 둔 모델에 있어서, 객체는 검증에 전용으로 사용되는 API를 통해 재생 또는 저장을 위한 호출을 허용한다. 런타임은, 객체에 의해 검증될 수 있는 권한 또는 식별자를 제공해야 한다. 예를 들면, 부모에 의한 시청제한은, 영화 콘텐츠의 서로 다른 부분을 나타내는 복수의 객체로 이루어진 그룹으로 구현될 수 있다. 또 다른 예로서, 전자 서적은 액세스 제한 요구사항과 그래픽 객체를 캡슐화할 수 있다.

도 2는, 자바공간(JavaSpaces) 아키텍처를 사용하는 지니 시스템(200)의 블록도이다. 자바공간은, 분산 운용체계를 생성하고, 자바 VM과 자바의 원격 방법 호출(RMI) 기능 뿐만 아니라, 자바 기반의 객체에 대한 저장고를 생성하는 아키텍처이다. 자바공간 구현은, 복수의 관련된 객체로 구성된 그룹을 저장하고, 지정된 피드에 대한 값-일치 탐색(value-matching look-up)에 근거하여 이들을 검색하기 위한 메카니즘을 제공한다. 이와 같은 구성은, 자바공간 서버가 원격 시스템 상에서 객체를 저장하고 검색하는데 사용될 수 있도록 한다. 자바공간 API는, 다수의 자바공간을 거쳐 다수의 동작을 단일 아토믹 동작으로서 동작하는 번들로 그룹화하는 기본 아토믹 트랜잭션(atomic transactions)을 제공하기 위해 특정한 패키지를 사용한다. 자바공간은, 다중 동작 및/또는 다중 공간 갱신이 아토믹으로 완료될 수 있도록 하는 트랜잭션 메카니즘을 지원한다. 용어 "아토믹성(atomicity)"은 트랜잭션 하에서 그룹화된 모든 동작이 발생하거나 어떠한 동작도 발생하지 않는다는 것을 의미한다. 지니는 장치의 네트워크 접속을 위해 마찬가지로 선 마이크로시스템즈(Sun Microsystems)에서 만든 기술이다. 지니는 네트워킹 PC들과 주변기기를 돕는 자바 기반의 소프트웨어 기술이다. 네트워크에 플러그되었을 때, 지니가 가능한 장치는 그것의 존재를 동보전송한다. 이 장치를 사용할 준비가 된 네트워크 클라이언트는, 서버 또는 네트워크 관리자를 바이패스함으로써, 장치 그 자체로부터 필요한 소프트웨어를 요구할 수 있다. 이와 같은 아키텍처는 현존하는 네트워크의 위에 세워진다.

시스템(200)은, 네트워크(208)를 통해 접속된 자바공간 서버(202, 204)와 클라이언트(206)를 구비한다. 자바공간 서버 202 또는 204는, 자바 프로그래밍 언어로 작성된 객체에 대해 분산된 지속성과 객체 교환 메카니즘을 제공한다. 객체들은 관련된 필드의 분류된 그룹화를 제공하는 항목에 기록된다. 클라이언트는, 새로운 항목을 기록하고, 현존하는 항목과 공간으로부터의 원격지의 항목을 탐색하기 위해, 자바공간 대해 간단한 동작을 수행할 수 있다. 이를 도구를 사용하여, 분산된 알고리즘을 구현하기 위해 데이터의 흐름을 사용하고 자바공간 시스템이 사용자에게 지속성을 구현하도록 하는 시스템에 기록할 수 있다. 관련된 요구가 존재할 때, 서버(202)는 (직렬화를 통해) 객체를 클라이언트(206)로 전송한다. 이와 같은 전송은 자바의 분산 전용사용 사양(Distributed Leasing Specification)에 의해 지정된 것과 같이 전용 사용에 해당한다. 허가과정은 이와 같은 허가를 한 사람에게 의해 명시적으로 취소될 때까지, 서비스 또는 자원을 허가하기보다는, 전용 사용의 자원 또는 서비스 허가는 시간에 기반을 둔다. 전용 사용에 대한 시간이 경과하면, 서비스가 종료하거나 자원이 비워진다. 이와 같은 "전용 사용"의 표현은 분산 시스템에서 특히 유용한데, 그룹의 구성성분 또는 접속의 실패로 인해, 통합되는 그룹의 서로 다른 부분은 통신을 할 수 없다. 도 2에 도시된 도면에 따르면, 서버(202)는 임시 저장을 위해 제 1 객체를 서버(204)에 전용으로 사용하게 하며, 임시 저장 또는 재생을 위해 제 2 객체를 클라이언트(206)에 전용으로 사용하게 한다. 이와 같은 구성은, 예를 들면, 주문형 비디오(오디오) 서비스 제공자, 다중 플레이어 비디오 게임 제공자 등에 적합하다. 이와 유사한 클라이언트-서버 아키텍처는, 윈도우즈 운영체제 상의 COM 클라이언트를 갖는, 마이크로소프트의 COM/DCOM 기술을 사용하여 구축될 수 있다.

KIPRIS(공개특허공보)

도 3은, COM/DCOM 서버(302)와 COM 클라이언트(304)를 갖는 시스템(300)의 도면이다. 서버(302)는 객체 액세스와 객체 저장을 제공한다. 클라이언트(304)는 COM 또는 DCOM 메커니즘을 사용하여 서버(302)를 액세스할 수 있다. 원격지에 대해서는, DCOM이 사용된다. 이와 같은 액세스 메커니즘은 클라이언트(304)에 대해 투명하다. COM 객체는 클라이언트(304) 상의 프로세스 내부에 전달되며, 원하는 콘텐츠를 생성하기 위해 관련된 API가 클라이언트(304)에서 호출된다. 객체는, 마이크로소프트의 디렉쇼(DirectShow) 콤포넌트와 같은 시스템 자원과 API에 대한 완전한 액세스를 갖는다.

도 4는 본 발명에 있어서 시스템(400)의 또 다른 구성을 나타낸 도면이다. 시스템(400)은, 객체를 제공하며 객체 저장고로서 기능을 수행하는 서버(402)를 구비한다. 이 시스템(400)은 클라이언트 404와 406을 더 구비한다. 시스템(400)은, 예를 들면, 화상회의에서와 같이 콘텐츠의 교환을 위한 다중 클라이언트 상호작용을 위해 사용된다. 콘텐츠 객체는, 클라이언트 404에 의해 서버/저장고(402)에 배치되며, 클라이언트 406에 의해 저장고(402)로부터 검색될 수 있다.

도 5는, 시스템(400)과 유사한 구성을 갖는 시스템(500)의 도면이다. 이 시스템(500)은 클라이언트(504, 506, 508, 510)에게 서비스를 제공하는 객체 서버(502)를 구비한다. 서버(502)는 다중 클라이언트 객체 상호작용을 가능하게 하기 위한 객체 저장고로서 기능을 수행한다. 콘텐츠 객체는, 클라이언트(504-510) 중에서 임의의 클라이언트에 의해 서버(502) 내부에 배치되며, 다른 클라이언트(504-510)에 의해 검색될 수 있다. 시스템(500)은, 클라이언트 514 및 516에게 서비스를 제공하는 중계 또는 복제 서버(512)를 구비한다. 콘텐츠 객체는, 클라이언트 504-510과 514-516의 우선순위 또는 액세스 특권에 근거하여 패키지화되거나 인터페이스를 노출할 수 있다.

더 상세한 정보를 위해서는, 당업계에서 입수할 수 있으며 참조를 위해 본 명세서 내부에 통합된, 선 마이크로시스템즈의 자바, 자바 공간, 지니 아키텍처와, 마이크로소프트의 콤포넌트 객체 모델(Component Object Model) 사양의 관련된 사양을 참조하기 바란다.

(57)청구의 범위

청구항1

런타임 환경(104)에서 정보의 최종 사용자 액세스를 위한 캡슐화된 프로시저(112)를 갖는 소프트웨어 객체(108)로 최종 사용자 콘텐츠 정보(110)를 제공하는 방법.

청구항2

제 1항에 있어서,
상기 프로시저는 콘텐츠 정보에 대한 조건부 액세스를 가능하게 하는 것을 특징으로 하는 방법.

청구항3

제 1항에 있어서,
소프트웨어 객체를 네트워크(208)를 통해 제공하기 위해 소프트웨어 객체를 직렬화하는 과정을 포함하는 것을 특징으로 하는 방법.

청구항4

제 1항에 있어서,
상기 객체는, 재생장치(104)에서 콘텐츠 정보를 재생할 수 있도록 하기 위한 프로시저를 포함하는 것을 특징으로 하는 방법.

청구항5

제 1항에 있어서,
상기 객체는 메모리(204; 206) 내부에 콘텐츠 정보의 저장을 가능하게 하기 위한 프로시저를 포함하는 것을 특징으로 하는 방법.

청구항6

제 1항에 있어서,
제공되는 내용은 전자 메일 서비스 내부에 포함된 것을 특징으로 하는 방법.

청구항7

제 1항에 있어서,
제공되는 내용은 원격회의 서비스 내부에 포함된 것을 특징으로 하는 방법.

청구항8

제 1항에 있어서,

KIPRIS(공개특허공보)

제공되는 내용은 화상회의 서비스 내부에 포함된 것을 특징으로 하는 방법.

청구항9

제 1항에 있어서,
상기 콘텐츠 정보는 오디오 정보를 포함하는 것을 특징으로 하는 방법.

청구항10

제 1항에 있어서,
상기 콘텐츠 정보는 비디오 정보를 포함하는 것을 특징으로 하는 방법.

청구항11

제 1항에 있어서,
상기 콘텐츠 정보는 영화를 포함하는 것을 특징으로 하는 방법.

청구항12

런타임 환경(104)에서 사용자가 콘텐츠 정보를 액세스할 수 있도록 하기 위한 프로시저를 포함하는 한 개 또는 그 이상의 소프트웨어 객체로서 콘텐츠 정보를 수신하는 방법.

청구항13

제 12항에 있어서,
객체 내부의 조건부 액세스 프로시저를 통해 콘텐츠 정보에 대한 조건부 액세스를 가능하게 하는 과정을 포함하는 것을 특징으로 하는 방법.

청구항14

제 12항에 있어서,
상기 콘텐츠 정보는 오디오 정보를 포함하는 것을 특징으로 하는 방법.

청구항15

제 12항에 있어서,
상기 콘텐츠 정보는 비디오 정보를 포함하는 것을 특징으로 하는 방법.

청구항16

제 12항에 있어서,
상기 콘텐츠 정보는 영화를 포함하는 것을 특징으로 하는 방법.

청구항17

제 12항에 있어서,
상기 콘텐츠 정보는 문자숫자식 정보를 포함하는 것을 특징으로 하는 방법.

청구항18

최종 사용자를 위한 콘텐츠 정보를 준비하고, 런타임 환경(104)에서 최종 사용자가 정보를 액세스할 수 있도록 하기 위한 캡슐화된 프로시저(112)를 갖는 소프트웨어 객체 내부에 콘텐츠 정보(110)를 패키징화하는 단계를 포함하는 방법.

청구항19

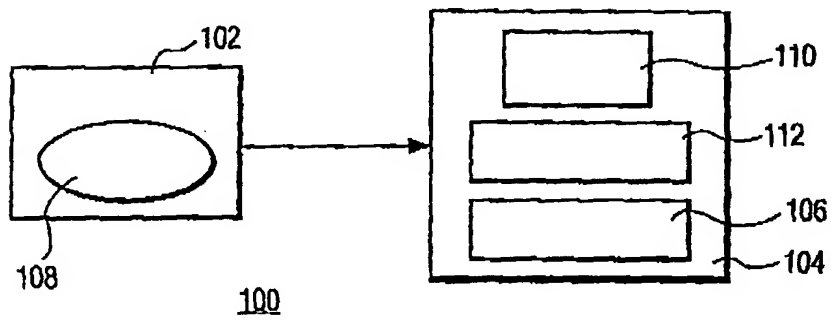
제 18항에 있어서,
상기 콘텐츠 정보는 영화를 포함하는 것을 특징으로 하는 방법.

청구항20

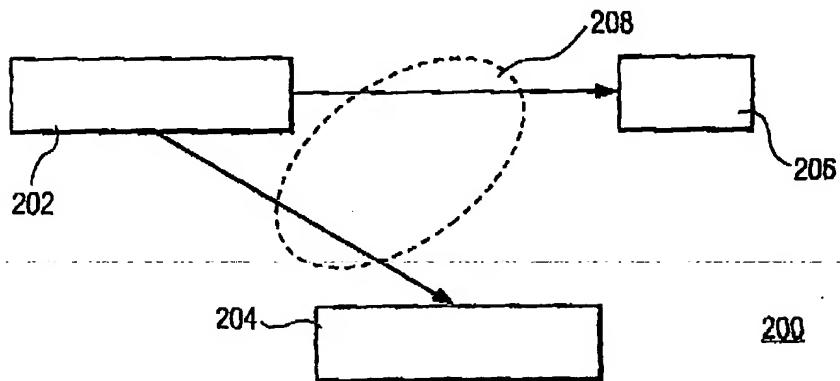
제 18항에 있어서,
상기 콘텐츠 정보는 문자숫자식 정보를 포함하는 것을 특징으로 하는 방법.

도면

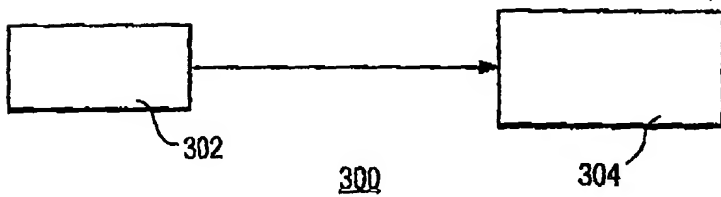
도면1



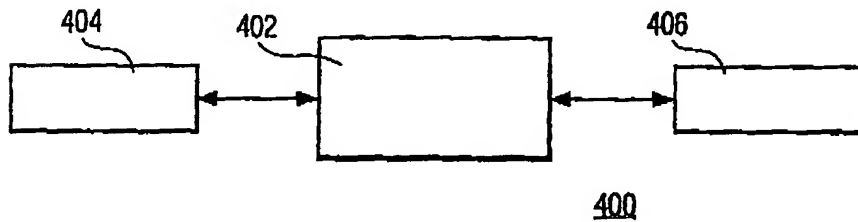
도면2



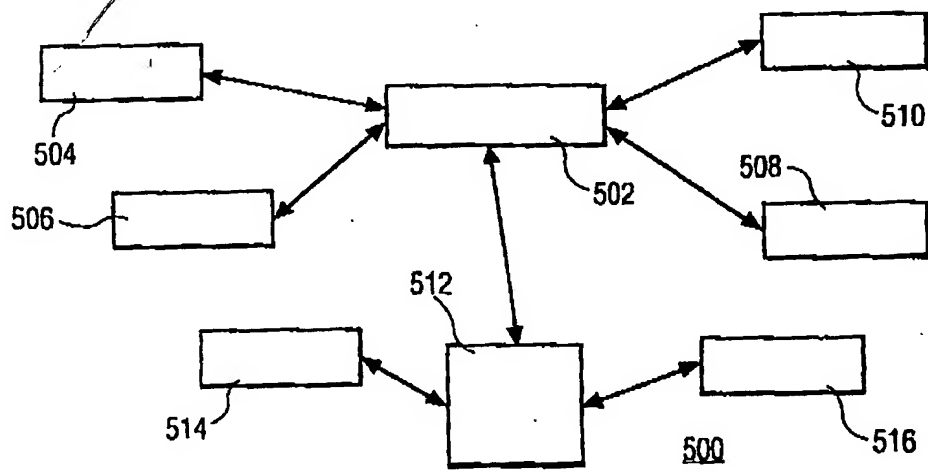
도면3



도면4



도면5



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.